

UNIVERSITÉ DE PICARDIE - JULES VERNE
École doctorale des sciences humaines et sociales

Mémoire en vue de l'habilitation à diriger des recherches en droit privé,
présenté et soutenu publiquement le 20 novembre 2017 par

Emmanuel NETTER

Numérique et grandes notions du droit privé

La personne, la propriété, le contrat

Garante : Madame le professeur Judith Rochfeld

devant un jury composé de :

Monsieur Bernard Beignier

Recteur de l'Académie d'Aix-Marseille,

Madame Valérie-Laure Bénabou

Professeur à l'Université d'Aix-Marseille,

Monsieur Daniel Mainguy

Professeur à l'Université de Montpellier,

Madame Sophie Pellet

Professeur à l'Université de Picardie – Jules Verne,

Madame Judith Rochfeld

Professeur à l'Université Paris 1 – Panthéon-Sorbonne,

Madame Célia Zolynski

Professeur à l'Université de Versailles – Saint-Quentin-en-Yvelines.

Remerciements

L’auteur remercie très vivement Madame le professeur Judith Rochfeld, qui lui a fait l’honneur de se porter garante du travail ici présenté ;

Mesdames et Messieurs les professeurs Bernard Beignier, Valérie-Laure Bénabou, Daniel Mainguy, Sophie Pellet et Célia Zolynski, pour avoir accepté de faire partie du jury ;

l’Université de Picardie – Jules Verne, de lui avoir accordé un semestre de congé pour recherches, sans lequel cet ouvrage n’aurait pas été le même ;

ses collègues, ses amis et sa famille pour leurs relectures, leurs conseils et leur soutien.

Liste des principales abréviations

AJ	Actualité jurisprudentielle
ACPR	Autorité de contrôle prudentiel et de régulation
<i>Adde</i>	Ajouter
Al.	Alinéa
<i>Alii</i>	Autres
AMF	Autorité des marchés financiers
ANSSI	Agence nationale de la sécurité des systèmes d'information
ARCEP	Autorité de régulation des communications électroniques et des postes
Art.	Article
BEREC	<i>Body of european regulators for electronic communications</i>
C. assur.	Code des assurances
C. com.	Code de commerce
C. conso.	Code de la consommation
C. pén.	Code pénal
CA	Cour d'appel
Cah. dr. de l'entreprise	Cahiers du droit de l'entreprise
CC	<i>Creative commons</i>
CCC	Contrats, concurrence, consommation
CCE	Communication commerce électronique
CEDH	Cour européenne des Droits de l'Homme
Cep.	Cependant
Cf.	Conférez
Chron.	Chronique
CJUE	Cour de Justice de l'Union européenne
CMF	Code monétaire et financier
CNCDH	Commission nationale consultative des droits de l'Homme
CNIL	Commission nationale informatique et libertés
CNNum	Conseil national du numérique
Coll.	Collection

Concl.	Conclusions
CSPLA	Conseil supérieur de la propriété littéraire et artistique
D.	Recueil Dalloz
Defrénois	Répertoire du notariat Defrénois
Dir.	Direction
DNS	<i>Domain name system</i>
Dr. et Patr.	Droit et patrimoine
DRM	<i>Digital rights management</i>
Éd.	Éditions
EFF	<i>Electronic frontier foundation</i>
Ex.	Exemple
FAI	Fournisseur d'accès à Internet
Fasc.	Fascicule
FCC	<i>Federal communications commission</i>
Gaz. Pal.	Gazette du Palais
GPL	<i>General public license</i>
HADOPI	Haute autorité pour la diffusion des œuvres et la protection des droits sur Internet
HTML	<i>Hypertext Markup Language</i>
IANA	<i>Internet Assigned Numbers Authority</i>
Ibid.	Au même endroit
ICANN	Internet corporation for assigned names and numbers
<i>In</i>	Dans
<i>Infra</i>	Ci-dessous
J.-Cl.	Juris-classeur
Jur.	Jurisprudence
<i>Loc. cit.</i>	À l'endroit précité
LPA	Les petites affiches
MTP	Mesures techniques de protection
NIR	Numéro d'identification au répertoire de l'INSEE
N°	Numéro
Not.	Notamment
NTIA	<i>National telecommunications and information administration</i>

Obs.	Observations
<i>Op. cit.</i>	Ouvrage précité
P.	Page(s)
PIN	<i>Personal identification number</i>
Préc.	Précité
Préf.	Préface
Rappr.	Rapprochez
RDBF	Revue de droit bancaire et financier
Rép. civ.	Répertoire de droit civil
Rép. com.	Répertoire de droit commercial
Rev. sociétés	Revue des sociétés
RFDA	Revue française de droit administratif
RJPF	Revue juridique personnes et famille
RLDA	Revue Lamy droit des affaires
RLDC	Revue Lamy droit civil
RLDI	Revue Lamy droit de l'immatériel
RSC	Revue de science criminelle
RTD. civ.	Revue trimestrielle de droit civil
RTD. com.	Revue trimestrielle de droit commercial
S.	Et suivant(s)
SMS	<i>Short message service</i>
Somm.	Sommaire
Spéc.	Spécialement
Ss.	Sous
<i>Supra</i>	ci-dessus
T.	Tome
TPC/IP	<i>Transmission Control Protocol / Internet Protocol</i>
TLS	<i>Transport Layer Security</i>
TOR	<i>The onion ring</i>
V.	Voyez
V°	<i>Verbo</i> (mot)

Sommaire

Première notion - La personne.....	41
Chapitre 1 - L'identité numérique.....	47
Section 1 - Les éléments de l'identité numérique.....	51
Section 2 - La protection de l'identité numérique.....	78
L'identité numérique : conclusion.....	144
Chapitre 2 - La communication électronique.....	146
Section 1 – La production de l'information.....	153
Section 2 - La canalisation de l'information.....	186
La communication numérique : conclusion.....	219
Deuxième notion - La propriété.....	221
Section 1 - Les infrastructures.....	225
Section 2 - Les contenus.....	256
Section 3 - Les terminaux.....	321
La propriété : conclusion.....	329
Troisième notion – Le contrat.....	333
Section 1 – Droit commun des contrats.....	336
Section 2 – Droits spéciaux des contrats.....	386
Le contrat : conclusion.....	418
Bibliographie.....	421

Introduction

« Governments of the Industrial World, you weary giants of flesh and steel, I come from Cyberspace, the new home of Mind. On behalf of the future, I ask you of the past to leave us alone. You are not welcome among us. You have no sovereignty where we gather. [...] »

Your legal concepts of property, expression, identity, movement, and context do not apply to us. They are all based on matter, and there is no matter here ».

John Perry Barlow, A Declaration of the Independence of Cyberspace, 1996¹.

1. Un nouveau monde. Un nouveau droit ? - Partout où la terre émerge des océans, les hommes ont pris pied. Ils ont occupé l'espace, constitué des nations. Ils se sont donné des gouvernements pour les diriger. Mais un continent nouveau serait apparu, mêlé de pensée et d'électrons, dans un à-côté, un ailleurs, un au-delà. Ses citoyens d'emprunt seraient voisins dans le monde des idées. Abstraits de leur assise terrestre, ils seraient par là dispensés d'obéir aux lois des hommes, attachées au sol. Telle est l'utopie proposée par John Perry Barlow, co-fondateur de l'*Electronic Frontier Foundation*, une association américaine de « défense des libertés publiques dans le monde numérique »². Le texte fut écrit en réaction à la promulgation, la veille, du *Telecommunications act* : cette loi visait notamment à adapter le droit américain des communications au développement d'Internet³.

La *Déclaration d'indépendance* est un texte controversé, y compris parmi les organisations non gouvernementales. L'*Information technology and innovation foundation* (ITIF) a ainsi publié en 2013 une réponse intitulée *Déclaration d'interdépendance du cyberspace*, dans laquelle on peut notamment lire :

1. - <https://www EFF.org/fr/cyberspace-independence>. Traduction proposée par E. Sadin, *La silicolonisation du monde. L'irrésistible expansion du libéralisme numérique*, éd. L'échappée, 2016, p. 61 : « Gouvernements du monde industriel, vous, géants fatigués de chair et d'acier, je viens du cyberspace, la nouvelle demeure de l'esprit. Au nom du futur, je vous demande à vous, du passé, de nous laisser tranquilles. Vous n'êtes pas les bienvenus parmi nous. Vous n'avez pas de souveraineté là où nous rassemblons. Vos concepts juridiques de la propriété et d'expression ne s'appliquent pas à nous. Ils sont issus de la matière, et il n'y a pas de matière là où nous sommes [...] ». V. les articles publiés à l'occasion des 20 ans du texte, par ex : A. Greenberg, « It's been 20 years since this man declared cyberspace independence », article *wired.com* du 2 août 2016 ; S. Gavois, « Il y a 20 ans, John Barlow publiait sa déclaration d'indépendance du cyberspace », article *nextinpact.com* du 8 février 2016.

2. - <https://www EFF.org/about/>.

3. - Le texte de la loi est consultable ici : <https://transition FCC.gov/Reports/tcom1996.pdf>.

You have no moral basis to declare the Internet a no-man's land of anarchy and lawlessness. The rights of man do not end where the Internet begins, nor should governments relinquish their duty to govern at the borders of cyberspace.

[...] you proudly proclaim that any ideas or property you can steal from others should be yours to reproduce and distribute freely in cyberspace. We reject the fiction that the Internet gives you the freedom to disregard basic human rights of property, expression, identity and movement. The rights to life, liberty and property are natural to man and preserved by the societies we build and the governments we elect⁴.

Aujourd'hui, l'idée selon laquelle Internet ne serait soumis à aucune loi n'est plus guère défendue⁵. En revanche, l'un et l'autre des deux textes posent la question de savoir si les concepts préexistants de droit privé, restés inchangés, demeurent habiles à régir ce monde nouveau - sont citées la propriété, l'identité ou encore la liberté d'expression. À supposer que des difficultés existent, elles ne seraient pas d'une nature exclusivement politique. Elles devraient, à l'évidence, être affrontées aussi par le juriste.

2. Cyberspace, Internet, numérique - Mais quel doit être précisément le champ des investigations ? Les deux « déclarations » se réfèrent au *cyberspace*, un mot apparu dans les années 80, sous la plume de l'auteur de science-fiction William Gibson⁶. Un juriste américain estime qu'il n'est pas synonyme « d'Internet » :

The Internet is a medium of communication. People do things “on” the Internet. Most of those things are trivial, even if important. People pay bills on the Internet, they make reservations at restaurants. They get their news from the Internet. They send news to family members using e-mail or IM chat. These uses are important in the sense that they affect the economy and make life easier and harder for those using the Internet. But they're not important in the sense that they change how people live [...].

Cyberspace, by contrast, is not just about making life easier. It is about making a different (or second) life. It evokes, or calls to life, ways of interacting that were not possible before. I don't mean that the interaction is new — we've always had communities; these communities have always produced something close to what I will describe cyberspace to have produced. But these cyberspace communities create a difference in degree that has matured into a difference in kind. There is something unique about the interactions in these spaces, and something especially unique about how they are regulated⁷.

4. - D. Castro, « A declaration of the Interdependance of Cyberspace », article *computerworld.com* du 8 février 2013. L'ITIF a été classée deuxième *think tank* le plus influent du monde dans le domaine « science dans technology » par un rapport de l'Université de Pennsylvanie : J. G. McGann, « 2014 Global Go To Think Tank Index Report » (2015) : http://repository.upenn.edu/cgi/viewcontent.cgi?article=1008&context=think_tanks.

5. - L. Lessig, *Code V2*, Basic Books, 2006, p. ix : « [Since the first edition of the book in 1999] [...] the confidence of the Internet exceptionals has waned. The idea—and even the desire—that the Internet would remain unregulated is gone ».

6. - V. la nouvelle *Burning Chrome* parue en 1982, puis le roman *Neuromancer* de 1984.

7. - L. Lessig, *Code V2*, *op. cit.*, p. 83.

En somme, Internet provoquerait, dans la manière qu'ont les hommes d'interagir, des modifications qui pourraient être ordonnées des plus marginales aux plus spectaculaires. Au-delà d'un certain seuil de nouveauté, la différence de degré se muerait en différence de nature ; le monde ancien ne serait plus seulement altéré : il serait chassé par un univers nouveau. Mais le point de bascule est nécessairement difficile à placer ; il est peut-être même d'ordre subjectif. De surcroît, si les évolutions profondes appellent plus sûrement des réactions de la part du système juridique, il n'est pas certain que les changements mineurs doivent rester sans effet. Les exemples cités en attestent, qui concernent la manière dont sont conclus des contrats ou échangées des informations. L'étude doit donc au minimum être élargie à Internet, plutôt que de se cantonner à un « cyberspace » au demeurant assez insaisissable.

Mais le réseau des réseaux est lui-même une excroissance d'un progrès technique plus vaste : la montée en puissance du traitement numérique de l'information. Lorsqu'il cherchait à faire comprendre la révolution qu'allait constituer, pour l'espèce humaine, la multiplication des ordinateurs, Steve Jobs avait parfois recours à la métaphore de la bicyclette. Une étude, expliquait-il, avait classé les animaux en fonction de l'efficacité avec laquelle ils se déplaçaient sur une distance d'un kilomètre. Une moindre dépense d'énergie se traduisait par un score plus élevé. L'humain dénué d'outil figurait dans le dernier tiers de la liste. Mais une fois à vélo, il prenait sans difficulté la tête du classement. Jobs ajoutait alors : « l'ordinateur est une bicyclette pour l'esprit »⁸. Le numérique a permis la construction de machines capables de résoudre des problèmes de plus en plus complexes. Mais son impact ne se limite pas au traitement de l'information : il concerne aussi sa circulation. La possibilité de réaliser une infinité de copies parfaites d'un fichier, à faibles coûts, a d'évidentes conséquences sociales et, partant, juridiques.

Il est nécessaire, avant d'aller plus loin, d'expliquer précisément ce qui constitue l'univers numérique (I). Nous verrons ensuite de quelles façons il entre en relation avec le monde du droit (II).

I - Le numérique

3. Brèves histoires du numérique - Il est possible, dans une certaine mesure, de retracer distinctement l'évolution des machines numériques (A) et celle de leur mise en réseau (B). Les

8. - M. Popova, « Steve jobs on why computers are like a bicycle for the mind (1990) », article *brainpickings.org* du 21 décembre 2011.

éléments historiques proposés seront nécessairement succincts, mais ils permettront une meilleure appréhension des objets techniques complexes que le droit est appelé à encadrer.⁹.

A - Les machines

4. Deux systèmes de représentation du monde — Lorsqu'une information sur le monde qui nous entoure doit être représentée — puis, éventuellement, manipulée —, deux systèmes sont concevables : l'analogique et le numérique. Selon un dictionnaire usuel, « analogique se dit d'une grandeur physique mesurée par une fonction continue ou d'un signal dont les variations sont continues »¹⁰. Au contraire, « numérique se dit de la représentation d'informations ou de grandeurs physiques au moyen de caractères, tels que des chiffres, ou au moyen de signaux à valeurs discrètes »¹¹. Des exemples permettront de mieux comprendre.

Supposons que le phénomène à retranscrire consiste dans la variation d'une température. Un thermomètre au mercure réalisera une représentation « par analogie » : le métal grimpera au sein d'un tube dans les mêmes proportions, de la même façon que la température qu'il mesure. Une grandeur physique (la hauteur de mercure) est substituée à une autre (la température). La modélisation n'aura pas de lacune : s'il y a eu passage progressif de cinq à douze degrés, le mercure aura occupé toutes les positions intermédiaires. Il aura, à un moment donné, représenté la température de 6,112 degrés, de même que celle de 9,763525 degrés : il n'y a pas d'autre limite à la finesse de la représentation que la capacité de l'observateur à la percevoir. L'information est « continue » ; elle est exhaustive. Imaginons à présent qu'un observateur scrute le thermomètre, et relève toutes les 5 secondes sa position : il en réalise un échantillonnage, en cristallisant l'information, ponctuellement, sous la forme d'un nombre - nécessairement un arrondi, dans notre exemple. L'information analogique a été numérisée, transformée en un nombre fini de symboles, qui se chargent de sens une fois interprétés, et se prêtent plus aisément à des opérations mathématiques que l'univers continu.

D'autres illustrations classiques peuvent être proposées. L'écoulement du temps peut être représenté analogiquement par une clepsydre : l'information matérialisée par le passage du fluide

9. - Sur l'histoire de l'informatique et d'internet, V. par ex. : E. Lazard et P. Mounier-Kuhn, *Histoire illustrée de l'informatique*, EDP sciences, 2016 ; P. Breton, *Une histoire de l'informatique*, éd la Découverte, 1987 ; J. Ryan, *A history of the internet and the digital future*, Reaktion books, 2010 ; E. C. Lallana et M. N. Uy, *The information age*, UNDP-APDID, 2003 ; G. Gromov, *Roads and crossroads of the Internet history* : http://www.netvalley.com/internet/history_of_internet.pdf ; V. Cerf et B. Aboba, « How the internet came to be », article netvalley.com, 1993.

10. - Dictionnaire Larousse en ligne, V° « Analogique ».

11. - *Ibid.*, V° « Numérique ». Une variable discrète ne peut prendre qu'un ensemble fini de valeurs.

sera continue. Si ce sont les vibrations d'un quartz stimulé électriquement qui sont utilisées pour fonder la régularité d'une horloge, il existe ensuite deux manières d'en tirer parti. Une trotteuse procédant à des rotations constantes autour d'un axe constitue un procédé analogique, tandis qu'un affichage numérique sera le produit d'un échantillonnage auquel on assignera une certaine précision - à la seconde, au milliardième de seconde. De même, la fréquence d'une note de musique ou l'intensité d'un son peuvent être converties en un courant électrique : il s'agit toujours de remplacer un phénomène physique par un autre, par analogie. On pourra alors représenter le résultat sous forme d'une courbe, parfaitement continue, sur un écran. Passer à une représentation numérique impliquera de changer la courbe en un nuage de points.

5. Calculateurs numériques et analogiques - Le lecteur contemporain, conscient du triomphe final du numérique sur l'analogique, pourrait croire que les deux techniques de représentation ont succédé l'une à l'autre au cours du temps, l'une étant moderne et l'autre archaïque. Ce serait une erreur : elles ont très longuement cohabité.

Elles sont aussi anciennes l'une que l'autre. Si l'on considère les machines à calculs les plus rudimentaires, le boulier appartient à la famille numérique : la réalité y est représentée par un ensemble fini de symboles, les boules. En revanche, le *mécanisme d'Anticythère*, daté du II^e siècle avant Jésus-Christ, était constitué d'un ensemble d'engrenages qui, en pivotant, proposaient une modélisation en continu de la course du soleil, de la lune et d'autres astres¹².

Avançons jusqu'au XVII^e siècle, et constatons que des calculatrices bien plus perfectionnées sont apparues dans l'un et l'autre groupe. La *Pascaline*, machine à additionner et soustraire les nombres jusqu'à six chiffres, imaginée par Blaise Pascal, appartient au monde numérique¹³. Presque au même moment apparaît la règle à calcul, instrument constitué de plusieurs échelles graduées coulissantes permettant non seulement de réaliser les opérations basiques, mais encore de calculer des racines carrées, cubiques, ou encore des logarithmes. Les mouvements des bandes les unes par rapport aux autres sont continus, et sont donc à classer dans l'univers analogique, même si au terme du processus l'œil de l'utilisateur va rechercher la graduation la plus proche du résultat et procéder à un arrondi – une sorte de numérisation par échantillonnage. L'instrument a été utilisé par les ingénieurs du monde entier jusque dans les années 1970¹⁴.

12. - E. Lazard et P. Mounier-Kuhn, *op. cit.*, p. 25.

13. - *Ibid.*, p. 36. Elle date de 1645. Quelques décennies plus tard, en 1664, Leibniz inventera une machine apte à la multiplication et à la division.

14. - *Ibid.*, p. 35.

L'analogique, de manière générale, n'est pas une technique de calcul plus faible ou plus lente que le numérique. Au contraire, face à des problèmes d'égale complexité, la résolution analogique a longtemps été beaucoup plus rapide. En effet, une fois qu'a été construit ou mis en place un système de représentation analogue au phénomène physique que l'on entend mesurer, il n'y a plus qu'à le faire fonctionner avec certaines valeurs d'entrée et à constater les valeurs de sortie, sans qu'il soit nécessaire d'analyser les détails du fonctionnement intermédiaire. Par exemple, pour connaître les caractéristiques aérodynamiques d'un appareil volant, il suffit d'en bâtir une maquette à petite échelle et de le placer en soufflerie : sans même qu'il soit nécessaire de modéliser, ni même de comprendre totalement les dynamiques à l'œuvre, il sera possible d'observer la réaction. À l'inverse, faire fonctionner une simulation, appelée par la pratique « soufflerie numérique », rend nécessaire la modélisation mathématique exhaustive du système, sa mise en équations complète. Il faut ensuite fournir les valeurs d'entrées à une machine numérique, qui procédera aux lourds calculs nécessaires à la restitution de valeurs de sortie.

Ainsi, les calculateurs analogiques constituaient un choix judicieux lorsqu'il fallait représenter une situation complexe, mais dont les grandes lignes étaient prévisibles à l'avance, et qu'il était nécessaire d'obtenir un résultat très rapide. En matière de balistique militaire, « l'ordinateur analogique » *Dumaresq* a longtemps été employé pour guider l'artillerie en situation de combat naval¹⁵. D'abord mécaniques, les ordinateurs analogiques sont peu à peu devenus électroniques, les ressorts et autres pistons étant remplacés par des inducteurs ou des résistances obéissant aux mêmes équations.

Malgré ses mérites, l'analogique a tout de même fini par être supplanté par le numérique en tant que machine à calcul.

6. Turing et le triomphe du numérique – Dès 1834, le mathématicien anglais Charles Babbage imagine une machine que beaucoup considèrent comme l'ancêtre de l'ordinateur. Mais c'est au cours de la Deuxième Guerre mondiale que l'intérêt pour ce type de machine, et, corrélativement, les moyens financiers alloués à leur fabrication va véritablement exploser. Le conflit fut en effet le théâtre d'un affrontement entre deux machines numériques : *l'Enigma* nazie et la « bombe » de l'anglais Turing¹⁶. Les armées allemandes utilisaient des communications chiffrées, c'est-à-dire incompréhensibles pour qui ne possédait pas un code secret. Il s'agissait d'un chiffrement par

15. - Son emploi est expliqué dans B.R. 1534, *Handbook on Minor Fire Control Instruments*, 1946 : <https://maritime.org/doc/br1534/>.

16. - E. Lazard et P. Mounier-Kuhn, *op. cit.*, p. 77. Le mot « bombe » vient des machines de cryptanalyse inventées préalablement par des équipes polonaises. Il aurait été inspiré par le cliquetis produit durant leur fonctionnement.

décalage, c'est-à-dire que chaque lettre du message « en clair » était déplacée d'un ou plusieurs rangs dans l'alphabet. Jules César utilisait déjà cette technique, mais il appliquait un décalage uniforme sur l'ensemble du message (par exemple, trois rangs vers le Z), terriblement rudimentaire. *Enigma* avait porté ce procédé à un très haut degré de sophistication.

Son utilisation était en apparence fort simple : l'opérateur saisissait son message « en clair » sur le clavier de la machine. Au fur et à mesure, des diodes s'allumaient pour indiquer quelles étaient les lettres constituant la version chiffrée. Ce résultat était obtenu par la circulation d'un courant électrique partant de la touche pressée et parvenant à la diode à allumer. L'objectif était de rendre ce parcours aussi complexe et difficile à prévoir que possible. Pour y parvenir, les ingénieurs allemands faisaient notamment transiter les électrons par des « rotors », des disques pivotants munis de contacteurs électriques¹⁷. Appliquer la clé de chiffrement — qui changeait tous les jours — consistait à placer chacun des rotors dans une certaine position avant d'entamer la saisie ou le déchiffrement du message. De surcroît, les rotors se déplaçaient au fur et à mesure de la frappe, l'un d'entre eux pivotant même à chaque pression d'une touche.

C'était donc une énigme numérique qui était posée : un ensemble fini de symboles (les lettres de l'alphabet) subissait une transformation mathématique (un décalage d'un ou plusieurs rangs). Il fallut une autre machine pour en venir à bout. Elle fut conçue à Londres, par une équipe de scientifiques dirigée par Alan Turing. Sa fonction était de tester à une vitesse effrénée les différents réglages possibles d'*Enigma*, en les appliquant aux messages chiffrés interceptés par les Alliés.

Mais si Turing est souvent considéré comme le père de l'informatique moderne, c'est peut-être davantage encore en raison de sa description du concept abstrait connu sous le nom de *machine de Turing*¹⁸. Il définit les contours théoriques d'une machine capable d'exécuter des calculs de toutes sortes lorsqu'elle est mise en œuvre à l'aide de langages de programmation adéquats. Alors que le calculateur analogique est spécialisé, et doit être reconstruit ou au moins reconfiguré à chaque fois qu'il doit résoudre un problème différent, l'ordinateur numérique est capable, sans subir aucune modification physique, de s'attaquer à une infinité de problèmes et de manipulations mathématiques de l'information. Dans l'après-Deuxième Guerre mondiale, c'était au prix d'une certaine lenteur dans l'exécution, mais l'augmentation exponentielle des puissances de calcul a fait peu à peu disparaître ce dernier inconvénient.

17. - En réalité, le fonctionnement était rendu plus complexe encore par l'utilisateur de pièces supplémentaires telles que le réflecteur et le tableau de connexions filiales. V. par ex. les explications fournies dans les biographies de Turing : A. Hodges, *Alan Turing ou l'énigme de l'intelligence*, trad. N. Zimmermann, Payot, 1988 ; E. Liberge et A. Delalande, *Le cas Alan Turing. Histoire extraordinaire et tragique d'un génie*, Les arènes BD, 2015.

18. - A. M. Turing, « On computable numbers, with an application to the Entscheidungsproblem » : https://www.cs.virginia.edu/~robins/Turing_Paper_1936.pdf.

Le numérique a également cet avantage sur l'analogique qu'il permet la reproduction à plusieurs reprises d'un ensemble de données sans perte de qualité, tandis que réaliser des copies de copies analogiques entraîne un affaiblissement progressif du signal, jusqu'à le rendre inexploitable¹⁹.

7. **L'informatique moderne** – L'histoire récente du calcul numérique ne sera esquissée qu'en quelques mots. En 1962, la place des ordinateurs dans les mondes de la recherche et des très grandes entreprises justifie qu'un mot nouveau soit inventé pour désigner les activités qui lui sont relatives. Deux Français proposent de fusionner « information » et « automatique » pour donner « informatique »²⁰. Aux USA, « *informatics* » aurait pu s'imposer de même, s'il n'avait pas été déposé par une société de développement de logiciels qui en interdit ensuite l'usage à tout autre²¹.

Lorsqu'il s'agit d'illustrer le développement de l'informatique personnelle, plusieurs appareils et dates peuvent être proposés. Nous retiendrons ici l'*Apple II* de 1977, en ce qu'il constituait la première machine vendue directement fonctionnelle – auparavant, les composants devaient être achetés séparément et assemblés, ce qui réservait l'utilisation des machines à un public éclairé²². Mais un matériel informatique bien conçu n'est rien sans logiciel lui conférant une utilité pratique : aussi faut-il mentionner le premier grand *best-seller* de l'industrie du secteur, sorti sur la machine d'Apple : *VisiCalc*, un tableur qui permit notamment aux petites entreprises de gérer avec une efficacité inédite leurs stocks ou leur comptabilité. De ce programme, on a pu écrire : « C'est une formidable accélération donnée à l'industrie micro-informatique. Tout un écosystème économique se met en place incluant éditeurs de logiciels, développeurs indépendants, boutiques de ventes grand public, magazines d'informatique... »²³.

Il n'est guère possible d'aller plus avant dans l'histoire de l'informatique sans se préoccuper de la mise en réseau des machines.

19. - En réalité, si le support des données numériques est endommagé, cela peut dégrader la copie voire la rendre impossible, mais il s'agit alors d'une limite accidentelle, qui n'est pas intrinsèquement liée au procédé. La précision est d'importance, puisque la fiabilité de long terme de nombreux supports, au premier rang desquels le CD-ROM, est actuellement remise en cause : Laboratoire national de métrologie et d'essais, dossier Longévité des disques enregistrables : mythe ou réalité ? : <https://www.lne.fr/fr/projets/gis-spadon/longevite-des-disques>.

20. - Il s'agissait de Philippe Dreyfus, ingénieur chez Bull, et de Robert Lattès, mathématicien travaillant pour le Commissariat à l'Energie Atomique : E. Lazard et P. Mounier-Kuhn, *op. cit.*, p. 77.

21. - *Ibid.*

22. - *Ibid.*, p. 202.

23. - *Ibid.*, p. 211.

B – Les réseaux

8. Première description théorique d'Internet – Chacun connaît le rôle joué, durant la Guerre froide, par la théorie de la *mutually assured destruction* (MAD), la destruction mutuelle assurée. Une attaque nucléaire américaine ou soviétique devait mener à une série de tirs de rétorsion entraînant la destruction des deux belligérants, en même temps que celle du reste de la planète. Si l'attaquant potentiel avait la certitude d'être puni en retour et de tout perdre, le bouton ne serait jamais pressé. Mais l'ensemble de cette doctrine était menacé par la faiblesse des réseaux de communication de l'époque :

A nuclear detonation in the ionosphere would cripple FM radio communications for hours, and a limited number of nuclear strikes on the ground could knock out AT&T's highly centralized national telephone network. (...) A key tenet of MAD was that the fear of retaliation would prevent either Cold War party from launching a first strike. This logic failed if a retaliatory strike was impossible because one's communications infrastructure was disrupted by the enemy's first strike²⁴.

C'est pour répondre à ces préoccupations qu'un chercheur du *think tank* américain *Research and Development* (RAND), Paul Baran, jeta en 1960 les bases théoriques d'un système préfigurant de manière frappante le réseau Internet²⁵. Plutôt que de transiter par un central, les informations sauteraient de nœud en nœud au sein d'un réseau décentralisé - tout en conservant la mémoire de la longueur du trajet parcouru afin que le chemin le plus court soit identifié et utilisé dès que possible²⁶. La destruction de nœuds entraînerait simplement la redirection des paquets par le meilleur chemin ensuite disponible. Pour parvenir à ce résultat, Baran proposait une alliance de deux disciplines, l'informatique et les télécommunications, qui semble constituer une évidence pour le lecteur contemporain, alors qu'elles étaient à l'époque tout à fait étrangères l'une à l'autre²⁷. Les ordinateurs permettaient d'apporter au réseau intelligence et réactivité.

Ces réflexions restèrent dans l'immédiat cantonnées à la sphère de la théorie militaire : les infrastructures imaginées n'existaient pas encore, et la compagnie de téléphone AT&T s'opposa activement à l'expérimentation d'un tel système²⁸.

24. - J. Ryan, *op. cit.*, p. 12.

25. - P. Baran, *Research memorandum on a distributed command and control system configuration*, RM-2632, 31 décembre 1960 : http://www.rand.org/content/dam/rand/pubs/research_memoranda/2009/RM2632.pdf.

26. - *Ibid.*, p. 32.

27. - J. Ryan, *op. cit.*, p. 14 : « (...) these were disciplines so mutually distinct that Baran worried his project could fail for lack of staff capable of working in both areas ».

28. - *Ibid.*, p. 15 : « When the Air Force approached AT&T to test Baran's concept, it "objected violently". There was a conceptual gulf between the old analogue paradigms of communication to which AT&T was accustomed and the centrifugal, digital approach that Baran proposed [...] ». La citation intercalée est issue d'une interview de P. Baran par D. Hochfelder, IEEE History Centre, p. 12.

9. **Première mise en œuvre** – De concept abstrait, le réseau décentralisé d'ordinateurs se muera en réalité concrète au sein d'une structure appelée *Advanced Research Projects Agency* (ARPA), agence civile au service du Pentagone, destinée à mutualiser les meilleurs talents des différentes armes (*Army, Navy, Air Force*) dans le domaine scientifique, sans leur assigner d'objectifs de court-terme susceptibles de brider leur créativité²⁹. Un projet d'amélioration des infrastructures de communication militaires vit le jour en 1967. L'influence éventuelle des travaux précurseurs de Baran n'est pas tout à fait claire ; toujours est-il qu'une direction similaire fut suivie : il s'agissait de bâtir un réseau capable de transférer des données découpées en petits paquets, de nœud en nœud, jusqu'à leur destination finale³⁰. Dès l'année suivante, un financement fut accordé pour la construction d'un réseau à quatre nœuds reliant les universités de Stanford, Santa Barbara, Los Angeles et de l'Utah³¹. C'est en effet dans les établissements d'enseignement supérieur et de recherche que se trouvaient les principales ressources informatiques civiles de l'époque. Ce lien entre Internet et le monde académique américain restera très fort par la suite. La première communication effective eut lieu le 29 octobre 1969. Elle a pu être relatée ainsi :

The plan was unprecedented: Kleinrock, a pioneering computer science professor at UCLA, and his small group of graduate students hoped to log onto the Stanford computer and try to send it some data. They would start by typing "login," and seeing if the letters appeared on the far-off monitor.

"We set up a telephone connection between us and the guys at SRI...", Kleinrock ... said in an interview: "We typed the L and we asked on the phone,

"Do you see the L ?"

"Yes, we see the L," came the response.

"We typed the O, and we asked, "Do you see the O ?"

"Yes, we see the O."

"Then we typed the G, and the system crashed"...

*Yet a revolution had begun*³².

En 1971, le réseau s'était étendu à quinze nœuds. L'ARPANET, le réseau de l'ARPA, préfigurait à l'évidence l'arrivée d'Internet, mais ne se confond pas avec lui. Il s'agissait en effet d'un réseau

29. - *Ibid.*, p. 23. En toute rigueur, l'armée américaine comprend encore deux branches, les *Marines* et les *Coast Guard*, mais leurs ressources scientifiques n'étaient pas du même ordre.

30. - *Ibid.*, p. 28. Les travaux de Baran furent semble-t-il découverts tardivement par Lawrence Roberts, le chercheur de l'ARPA chargé du projet. Baran fut cependant consulté par la suite.

31. - *Ibid.*, p. 28.

32. - G. Gromov, *op. cit.*, p. 4.

homogène, conçu et mis en œuvre de bout en bout par les mêmes équipes, tandis qu'Internet est une curieuse créature de bric et de broc.

10. Bâtir Babel : l'invention des protocoles de communication – Permettre un dialogue non seulement entre ordinateurs au sein d'un même réseau, mais aussi entre réseaux distincts, inventer une langue commune à tous, était la condition de l'apparition d'Internet. La tâche fut initialement confiée à un simple groupe de *graduate students* disséminé dans les diverses universités financées par l'ARPA. Les techniques et l'ambiance de travail adoptés méritent d'être évoqués en quelques mots, car ils sont décrits par les historiens du réseau comme « ayant donné le ton pour le développement de la future culture Internet »³³. L'étudiant ayant initié la discussion ne pouvant se prévaloir d'aucun titre ni d'aucune position hiérarchique, il intitula modestement son message « *request for comments* » (RFC), soit « appel à commentaires »³⁴. Les RFC sont devenus par la suite les documents officiels décrivant le fonctionnement technique d'Internet³⁵. Leur élaboration obéit à un processus dont la philosophie générale n'a pas varié depuis : « *rough consensus and running code – that means we don't really vote exactly, we just try to assess rough consensus among the group trying to agree on proposed standard* »³⁶. À la lumière de ces éléments, le mode de fonctionnement d'une institution contemporaine comme l'ICANN, abordé plus loin dans l'étude, se comprendra plus aisément³⁷. Les premiers travaux du groupe donnèrent naissance au *Network Control Protocol* (NCP), qui permettait aux machines de dialoguer au sein de l'ARPANET.

Restait à connecter les réseaux entre eux : à côté du réseau filiaire ARPANET, existaient en effet au milieu des années 70 le réseau radio PRNET, ainsi que le réseau satellite SATNET³⁸. En 1974, une équipe dirigée par Vinton Cerf mit au point cette langue commune qui marquerait la naissance du réseau des réseaux : le *Transmission Control Protocol* (TCP). Le RFC destiné à décrire cette norme technique fait apparaître, dans son titre, un mot nouveau, abréviation d'*inter-networking* : Internet³⁹. Un autre protocole fut conçu, l'*Internet Protocol* (IP), dont l'objectif n'est pas de permettre la communication entre réseaux, mais de fournir à chaque machine connectée une adresse

33. - J. Ryan, *op. cit.*, p. 31.

34. - S. Crocker, « Request for comments 1. Host software » : <http://tools.ietf.org/html/rfc1>.

35. - V. la RFC 2555, « 30 years of RFCs » : <http://tools.ietf.org/html/rfc2555>.

36. - Vint Cerf, membre du premier groupe de travail (et futur vice-président de Google), cité dans J. Ryan, *op. cit.*, p. 32 (email à l'auteur). Cette connexion à une machine distante constituait l'objectif — non atteint — du premier test d'octobre 1969 relaté plus haut.

37. - V.infra, n°203.

38. - J. Ryan, *op. cit.*, p. 36.

39. - RFC 675, « Specification of internet transmission control program » : <http://tools.ietf.org/html/rfc675>.

unique permettant de l'identifier comme émetteur et receveur d'informations⁴⁰. Son importance était également fondamentale.

L'ensemble appelé TCP/IP est toujours à la base du fonctionnement d'Internet, et a été mis gratuitement à la disposition de tous par ses inventeurs.

11. Du réseau aux usages - Un des principes fondateurs d'Internet veut que l'infrastructure de communications et les protocoles TCP/IP transportent les paquets de données de manière aveugle, sans aucun égard pour leur contenu exact. Nous y reviendrons longuement, notamment en abordant le principe de « neutralité du réseau », qui fait actuellement l'objet de vifs débats⁴¹. Le mot « Internet » désigne donc, dans un sens strict, uniquement un véhicule de l'information, mais non les finalités de ce transport. Certains usages ont été inventés au temps d'ARPANET ; d'autres sont plus récents ; n'importe qui peut en imaginer de nouveaux à chaque jour qui passe. Ils prennent la forme de protocoles supplémentaires, relevant de la « couche applications », qui fonctionnent au-dessus des protocoles de la « couche communication ».

Une des premières possibilités d'utilisation d'ARPANET avait consisté à utiliser un autre terminal informatique à distance. Soit un chercheur qui se trouve dans une université A, mais qui souhaiterait utiliser la puissance de calcul bien supérieure disponible dans l'université B. Il pouvait utiliser le réseau pour s'identifier sur la machine de B et en prendre le contrôle depuis les locaux de A⁴².

Très rapidement (dès 1971), un protocole de transfert de fichiers (*File Transfert Protocol* ou FTP) est mis au point, qui permet notamment de rapatrier un fichier présent sur l'ordinateur B vers l'ordinateur A sans avoir besoin de s'identifier sur cette machine distante⁴³.

La messagerie électronique, ou email, est inventée seulement un an plus tard, et rencontre un succès tel qu'elle représente presque aussitôt l'essentiel du trafic⁴⁴.

En revanche, l'invention du *World Wide Web* (www) est bien plus récente. Elle résulte de l'intervention du protocole *Hypertext Markup Language* (HTML) par le Britannique Tim Berners-

40. - RFC 791, « Internet protocol. DARPA Internet program protocol specification » : <http://tools.ietf.org/html/rfc79>.

41. - V.infra, n°191.

42. - J. Ryan, *op. cit.*, chap. 6, citant un email de Leonard Kleinrock adressé à l'auteur.

43. - RFC 114, « A file transfert protocol » : <https://tools.ietf.org/html/rfc114>. « [FTP] does not require that you explicitly log into a remote system or even know how to "use" the remote system. An intermediate process makes most of the differences in commands and conventions invisible to you. For example, you need only know a standard set of network file transfer commands for your local system in order to utilize remote file system ».

44. - J. Ryan, *loc. cit.*

Lee⁴⁵. Le HTML a permis d'agencer des informations telles que du texte, mais aussi des images, des vidéos, des sons, sous la forme de « pages Web ». C'est également ce protocole qui permet de relier des éléments d'une page à la fois entre eux (par le biais d'un lien hypertexte interne) et à des ressources tierces (par l'intermédiaire d'un lien hypertexte externe). Ce protocole a longtemps été mis en œuvre de manière exclusive par des logiciels généralistes, les navigateurs, mais il est aujourd'hui largement employé par des programmes spécialisés, les applications, en particulier sur les téléphones intelligents. Ainsi, « le Web » représente un usage particulier « d'Internet », à strictement raisonner.

Toutefois, il est très courant d'utiliser le mot « Internet » comme un raccourci pour désigner des usages du réseau, et les développements qui suivront ne se priveront pas d'utiliser ainsi le terme lorsque cela ne présentera aucun danger particulier de confusion sur le plan technique.

Ainsi s'achève une première présentation, rudimentaire, des progrès que l'on peut regrouper sous le concept de « technologies numériques ». Des compléments ou approfondissements seront proposés au fil de l'étude, en tant que de besoin.

Il est temps de proposer une première description des relations qu'entretient le monde du numérique avec celui du droit.

II - Le numérique et le droit

12. Trois types de rapports - Certains auteurs n'hésitent pas à qualifier la progression des technologies numériques de « troisième révolution industrielle »⁴⁶. Il est vrai que la maîtrise de la vapeur, puis celle de l'électricité et du pétrole, avaient ceci en commun qu'elles avaient entraîné une transformation globale de la société des hommes. Elles avaient placé au service des industries comme des particuliers des armées d'esclaves mécaniques, décuplant la productivité des usines, réduisant les distances à la surface du globe, augmentant, au sein des foyers, le confort de vie et le temps dévolu aux loisirs⁴⁷. Mais les progrès des ordinateurs ainsi que des réseaux informatiques ont

45. - V. not. T. Berners-Lee, *Weaving the web : the original design and ultimate destiny of the World wide web by its inventor*, Harper San Francisco, 2000. Sur le contexte ayant entouré cette création, V. aussi infra, n°199.

46. - J. Rifkin, *La troisième révolution industrielle*, Actes sud, 2013. L'auteur estime que les progrès du numérique et ceux des énergies renouvelables vont s'entremêler pour faire entrer notre société dans une ère nouvelle. Pour une critique de cette théorie (et du concept même de « révolution industrielle » comme outil d'analyse historique, en tant qu'il représente comme des « moments » des évolutions qui sont en réalité de long terme), V. par ex. D. Bourg et al., « “La Troisième Révolution” de Rifkin n'aura pas lieu », article *Liberation.fr* du 21 octobre 2014.

47. - « À travers sa consommation d'énergie, chaque Européen dispose désormais de 100 domestiques en permanence, qui s'appellent machines d'usine, trains et voitures, bateaux et avions, tracteurs, chauffage central, électroménager, tondeuse à gazon et téléskis » : J.-F. Mouhot, *Des esclaves énergétiques*, éd. Champ Vallon,

eux aussi un impact global. La force procurée aux individus se situe certes sur le plan immatériel plutôt que tangible. Les capacités qui leur sont conférées consistent à produire, comprendre, analyser, trouver, projeter au loin des informations comme jamais ils n'avaient pu le faire auparavant⁴⁸. C'est donc l'intelligence de la société humaine qui se trouve renouvelée, au sens littéral : les instruments par lesquels elle observe le monde, se forme une opinion de lui, en propose un discours. L'ensemble des interactions humaines s'en trouve potentiellement altéré : on pressent dès lors que le droit, en tant qu'il constitue une « grammaire de la société », sera sommé d'évoluer dans de nombreux domaines - ce qui ne signifie pas, tant s'en faut, que toutes ces injonctions méritent obéissance.

Les points de contact du droit et des progrès informatiques seront donc nécessairement innombrables. Proposons toutefois une première esquisse de leurs rapports, d'où il résulte que le numérique peut se trouver dans une relation de collaboration (A), de concurrence (B) ou de soumission (C) avec le droit.

A - Les rapports de collaboration

13. **Plan** - Le numérique est d'un secours particulier aux professions dans lesquelles la manipulation d'information occupe une place prépondérante. À l'évidence, les métiers du droit obéissent parfaitement à cette définition. Le plaideur, l'avocat, le juge, le notaire, l'huissier : tous consultent des textes et en rédigent, tous tiennent des discours sur ce qui est souhaitable ou sur ce qui va advenir. Il y a plusieurs décennies que le numérique améliore les processus de circulation de ces informations (1). Mais un mouvement plus récent, et plus controversé, lui confère des responsabilités supérieures : celles de préparer une décision humaine (2) voire même d'agir en toute autonomie (3).

1. - L'accès à l'information

14. **Mieux connaître la norme** - Il y a près de vingt ans, Pierre Catala publiait un ouvrage visionnaire, en bonne partie consacré aux bouleversements des techniques de documentation juridique entraînés par la numérisation⁴⁹. Décrivant « l'étrange couple formé par l'hermine et la puce », il y affirmait que les banques de données juridiques allaient « influencer l'évolution du

2011, p. 10, citant J.-M. Jancovici et A. Grandjean, *Le plein s'il vous plaît !*, Seuil, 2006.

48. - Pour voir quelle somme de données est produite en une minute d'activité par les grandes plateformes opérant sur Internet : J. James, « Date never sleeps 4.0 », article *domo.com* du 28 juin 2016.

49. - P. Catala, *Le droit à l'épreuve du numérique. Jus ex machina*, PUF, 1998.

droit » en améliorant significativement la connaissance de ses sources⁵⁰. Le phénomène d'inflation normative, maintes fois décrit, est accompagné d'une inflation doctrinale qui fait aujourd'hui du droit un continent impossible à parcourir à pied. La consultation de sources et d'index exclusivement reproduits sur papier multiplie les déplacements, les manipulations, introduit une pesanteur qui n'est plus guère compatible avec le rythme frénétique imprimé aujourd'hui au monde des juristes - on peut le regretter. Mais le numérique ne s'est pas contenté d'accélérer le processus de consultation : la puissance des moteurs de recherche attire l'attention du chercheur sur des sources qu'il aurait probablement manquées, en dépit de son expérience.

Mieux encore : l'informatique ne se contente pas d'offrir un dépouillement plus rapide et plus exhaustif d'un corpus resté inchangé. Elle ouvre la possibilité de faire croître la masse d'informations de manière exponentielle sans mettre le juriste à genoux. Le numérique a-t-il fourni les moyens de résister à un torrent furieux qui se serait écoulé même sans lui... ou est-il à l'origine du problème ? Pierre Catala opte pour une vision optimiste du phénomène.

Du côté de l'informatique, on opposera les banques de données qui compilent des documents édités, c'est-à-dire inscrits sur des supports traditionnels, à celles qui traitent des sources inédites. Les premières augmentent la commodité, la rapidité, la sécurité de l'accès à des données dont la masse rend la consultation malaisée et aléatoire. Les secondes comportent les mêmes avantages, mais elles apportent, en outre, à l'usager un surcroît d'information qui peut être immense. Celles-ci, en dévoilant des réalités naguère inconnaissables (en jurisprudence, notamment), pourraient modifier insensiblement l'équilibre des sources du droit, ce que les premières ne sauraient faire. À tout le moins, un bon usage des banques de données élèvera le niveau de la connaissance juridique, ce qui nous conduit du côté du droit⁵¹.

Le Code de l'organisation judiciaire a été récemment enrichi d'une disposition qui va parfaitement en ce sens : « [...] les décisions rendues par les juridictions judiciaires sont mises à la disposition du public à titre gratuit dans le respect de la vie privée des personnes concernées »⁵². À l'ère du papier, seule une fraction des décisions de la Cour de cassation était publiée. Le numérique permet depuis plusieurs années qu'elles le soient toutes, mais s'y ajouteront bientôt tous les arrêts de cours d'appel et, surtout, l'énorme masse des décisions rendues par les juridictions du premier degré. Les supports traditionnels ne permettaient pas le stockage de tels matériaux en bibliothèque, sans même parler de leur exploitation fructueuse. La démarche s'inscrit dans un mouvement plus large d'*open data*, initié par la loi dite « République numérique », c'est-à-dire de mise à disposition

50. - P. Catala, *op. cit.*, chap. 12 : « les banques de données juridiques peuvent-elles influencer l'évolution du droit ». L'expression « l'hermine et la puce » figure au n°1.

51. - *Loc. cit.*

52. - Art. L. 111-13 du Code de l'organisation judiciaire, issu de la loi n° 2016-1321 du 7 octobre 2016 pour une République numérique.

du public des données d'intérêt général, en particulier celles produites par les administrations⁵³. Elle constitue « un défi technique », notamment si l'on souhaite anonymiser les décisions ainsi publiées de manière irréversible⁵⁴. Parmi les effets bénéfiques escomptés de cette mise à disposition, le Premier président de la Cour de cassation cite une meilleure harmonisation des décisions au niveau national, les juges du fond étant mis en mesure de se lire les uns les autres, mais aussi un développement des modes alternatifs de règlement des litiges, dans la mesure où les avocats des parties pourraient plus facilement anticiper la décision à venir, et s'en inspirer par exemple dans la rédaction d'une transaction⁵⁵. Le haut magistrat rejoint donc Pierre Catala pour estimer que lorsque le droit est mieux connu, il s'en trouve ensuite amélioré par un choc en retour. On relève en revanche que les simples citoyens ne sont pas cités parmi les destinataires prioritaires de cette mise à disposition, et ce à juste titre. Il est évident qu'il ne suffit pas de mettre les sources primaires à portée de clic du non-juriste pour que celui-ci soit en mesure de les comprendre sans l'assistance d'un professionnel. L'objectif consistant à rendre les règles essentielles de la vie en société plus intelligibles à tous est évidemment fondamental. Mais la simple mise à disposition d'un matériau brut n'y participe pas, ou peu.

En revanche, l'amélioration du processus de création de la loi pourrait y contribuer. Certains souhaitent que le numérique soit sollicité en ce sens.

15. Mieux concevoir la norme - Nous avons vu que la loi « République numérique » avait cherché à amplifier un mouvement ancien tirant parti des technologies informatiques pour faciliter l'accès aux règles de droit. Mais avant cela, le Gouvernement avait donné aux internautes, pour la première fois, la possibilité de donner leur opinion sur ce que devrait être le contenu même de cette réforme. Autrement dit, il s'agissait de faire jouer un rôle au numérique en amont de la norme, au sein du processus menant à son adoption, et plus seulement en aval, pour faciliter sa connaissance et sa mise en œuvre par les professions du droit. Un site Internet a été mis en place, qui permettait à toute personne connectée à Internet de discuter des termes du projet de loi, d'en proposer des amendements, et de voter sur ceux soumis par d'autres citoyens. Il eût été impossible d'ouvrir une salle de réunion à l'ensemble des Français intéressés, si ses murs n'avaient été virtuels.

53. - V. not. *La jurisprudence dans le mouvement de l'open data. Actes du colloque à la Cour de cassation, 14 octobre 2016*, JCP G, 2017, n° 9, supplément n° 1.

54. - L. Cadiet (dir.), *L'open data des décisions de justice. Mission d'étude et de préfiguration sur l'ouverture au public des décisions de justice*, Rapport à Mme la garde des Sceaux, ministre de la Justice, novembre 2017.

55. - B. Louvel, « Allocation du Premier président Bertrand Louvel » in *la jurisprudence dans le mouvement de l'open data. Actes du colloque à la Cour de cassation, 14 octobre 2016*, JCP G, 2017, n° 9, supplément n° 1.

Plus de 21000 contributions ont ainsi été enregistrées, 8500 « arguments, amendements et propositions », 150000 votes⁵⁶. Le Gouvernement s'était engagé à répondre aux propositions les plus populaires — celles ayant recueilli le maximum de votes de soutien -, selon une logique inspirée de celle des réseaux sociaux. Si la doctrine a salué le procédé dans son principe, elle a cependant appelé à la vigilance face aux modalités de mise en œuvre⁵⁷. Il fut relevé qu'un petit nombre d'utilisateurs très motivés avait été à l'origine de l'essentiel de l'activité de la plateforme de consultation⁵⁸. Cela n'est pas nécessairement un problème : ce peut être l'occasion pour certains foyers d'expertise de la société civile d'ajouter leurs compétences à celles qui résultent du processus législatif classique. Mais, en l'état, il est clair que ce n'est pas « la » population française qui participe à ce processus de « co-rédaction ». Par ailleurs, le procédé n'a d'intérêt que si des moyens étatiques suffisants sont alloués pour examiner sérieusement les propositions populaires et, au besoin, leur donner un tour technique plus solide, sans pour autant en trahir l'esprit⁵⁹. Enfin, quand bien même les suggestions citoyennes seraient reprises dans le projet de loi soumis au Parlement, elles n'auront eu qu'un intérêt restreint si la représentation nationale et le Gouvernement s'en débarrassent au fur et à mesure du processus législatif. La loi République numérique n'a pas tout à fait évité cet écueil⁶⁰.

Malgré ce premier résultat en demi-teinte, d'autres idées émergent pour renouveler la démocratie représentative en exploitant des outils numériques, au sein des processus électoraux comme dans le travail législatif : c'est le mouvement dit des *civic tech*⁶¹. Dans un avis récent, le Conseil National du numérique propose quelques pistes pour l'avenir⁶². En faveur d'une plus grande transparence, il suggère de « publier les comptes de campagne des candidats et l'utilisation de [l'indemnité

56. - www.republique-numerique.fr.

57. - V. not. V. Lasserre, « Investiture de la société civile au Parlement. Analyse d'une nouvelle méthode législative », *JCP G*, 2016, n° 7, 181 ; A. Denizot, « La loi pour une République numérique : tous législateurs ? », *RTD. civ.*, 2017, p. 232.

58. - A. Denizot, art. préc. : « Enfin, et même si on peut s'enthousiasmer des chiffres de participation, n'oublions pas non plus qu'elle a été très inégale, la plus grande partie des contributions étant le fait de quelques-uns. Ainsi, les treize premiers contributeurs déclarés citoyens totalisent seuls plus de 10 000 actions sur la plateforme, alors que 10 353 citoyens ont eu moins de neuf contributions (dont environ 5 000 citoyens avec une seule contribution) [...] ».

59. - Sur cette question de la communication et du traitement des informations : V. Lasserre, art. préc.

60. - V. par ex. dans le chapitre II, « économie du savoir », la section 1 sur « Les communs » : <https://www.republique-numerique.fr/project/projet-de-loi-numerique/consultation/consultation>. Les propositions fortes et très soutenues qui s'y trouvaient n'ont pas connu de postérité législative.

61. - F. Schott, « Les "civic tech" ou le b.a-ba de la démocratie 2.0 », article *lemonde.fr* du 26 avril 2017. L'article évoque par exemple le site LaPrimaire.org, qui visait « faire émerger un candidat de la société civile dans la course à l'Élysée ».

62. - CNNum, *La confiance dans la vie publique, avec et pour les citoyen-ne-s d'une société numérique*, avis de juillet 2017.

représentative de frais de mandat] par les parlementaires en open data », de « transformer les réserves parlementaires en 577 appels participatifs » ou encore de rendre publics les agendas des représentants, en signalant en particulier leurs rendez-vous avec des lobbies⁶³. Pour améliorer la qualité de la loi, il souhaite « faire des contributions citoyennes sur les projets de loi un principe, en donnant au Gouvernement la responsabilité de justifier les exceptions », mais aussi « permettre à des communautés [...] de déposer des amendements citoyens, et d'être assisté par un administrateur pour arriver à la bonne expression formelle »⁶⁴.

Tous les procédés qui viennent d'être présentés visent à donner accès à ceux qui sont intéressés par la conception ou l'application du droit à un vaste ensemble d'informations pertinentes. Certaines préexistaient à la numérisation, mais étaient d'un maniement plus long et difficile ; d'autres n'existeraient simplement pas sans le recours à l'informatique et aux réseaux. Mais les nouvelles technologies peuvent être mises au service du droit d'une manière plus spectaculaire encore.

2 - L'analyse de l'information

16. L'aide à la décision - Les techniques mentionnées jusqu'ici reposaient principalement sur la dématérialisation : il s'agissait d'apporter, sur le bureau virtuel du parlementaire, la contribution de milliers de citoyens ; sur celui de l'avocat ou du juge, la sagesse de tous les tribunaux de France. Ces progrès réservaient bien une certaine place au traitement de l'information. Pour faire émerger les amendements les plus populaires parmi les internautes, un algorithme les ordonnait selon le nombre de votes qu'ils avaient recueilli. Pour que le professionnel trouve la décision la plus proche du dossier qu'il avait à traiter, un moteur de recherche était mis en œuvre, sans lequel un stock de trois millions de jugements et d'arrêts n'avait aucune utilité.

Mais laissons à présent les algorithmes monter en puissance, et passer de l'ombre à la lumière. C'est une chose que d'apporter à l'avocat, à partir d'un mot-clé, un fascicule de doctrine, un arrêt de cassation et deux jugements de TGI, qu'il appartiendra à l'homme de loi d'exploiter. C'en est une autre, pour l'ordinateur, de mobiliser par lui-même ces éléments afin d'évaluer l'opportunité d'agir en justice, les chances de succès et les dommages-intérêts probables, ou de proposer un modèle de contrat ou de transaction. De maçon, le voici architecte. Il y a encore dix ans, cette perspective

63. - *Ibid.*, recommandations 1, 3 et 4. Nous faisons figurer un simple échantillon des recommandations, sans nier en rien les mérites de celles qui ne sont pas reprises. Il est à noter que la pratique des « réserves parlementaires » a pris fin, depuis, en vertu de la loi organique n° 2017-1338 du 15 septembre 2017 pour la confiance dans la vie politique, art. 14 s.

64. - *Ibid.*, recommandations 7 et 9.

aurait fait sourire, tant elle semblait lointaine alors. Et pourtant, voici comment une société du secteur des *legal tech* présente actuellement ses services :

À l'occasion de votre prochaine procédure, allez-vous « gagner » ? Allez-vous « perdre » ? Et quels seront les montants décidés par le juge ? On se dit souvent qu'avec un bon dossier, on gagne et qu'avec un mauvais, on perd. C'est souvent vrai, mais ce n'est pas si simple ! Au-delà des compétences de l'avocat, il y a l'aléa judiciaire [...] Avec nos outils, qui utilisent des techniques de pointe en machine learning (intelligence artificielle) et associent compétences mathématiques et juridiques, vous pouvez cependant anticiper de manière fiable et réaliste cette part d'aléa⁶⁵.

Un magistrat associé au projet s'exprime même en ces termes :

J'étais sceptique au départ, car notre manière de raisonner est différente, mais j'ai pensé qu'il valait mieux anticiper et accompagner l'arrivée de l'intelligence artificielle, déjà présente ailleurs, dans le droit. Je me suis aussi dit que je pouvais mettre mon expérience de praticien de la justice au service de son travail, dont je connais l'exigence. Et puis, dans un contexte où les tribunaux sont très chargés, l'idée était d'apporter des anticipations fiables de ce qui attend les justiciables, pour qu'ils aient, s'ils le souhaitent, la possibilité de négocier efficacement sans nécessairement passer par un tribunal⁶⁶.

Ainsi, l'algorithme ne se contente pas de rassembler les briques élémentaires qui seront ensuite placées au service du raisonnement humain. Il bâtit par lui-même, en usant d'ailleurs d'autres méthodes. L'homme de loi formalisait un raisonnement. L'algorithme fonctionne par induction suivie de déduction, en relevant des analogies entre l'exercice qui lui est demandé — analyser les chances de telle action en justice, rédiger un contrat réglant telles difficultés concrètes — et la myriade d'exercices similaires menés à bien, par le passé, par des esprits humains⁶⁷. Ces évolutions vont remettre en question, pour commencer, les fonctions de secrétaire ou d'assistant : toutes les tâches un tant soit peu répétitives qui pourront être menées aussi bien, sinon mieux, par la brutale puissance de l'analogie informatique que par l'esprit plus subtil de l'homme. Resteront seuls à leurs postes ceux qui disposent du plus haut degré d'expertise. Ils seront aptes à prendre la décision finale

65. - <http://caselawanalytics.com/>. Sur ces questions, V. not. A. Garapon, « Les enjeux de la justice prédictive », *JCP G*, 2017, doctr. 31 ; B. Dondero, « Justice prédictive : la fin de l'aléa judiciaire ? », *D.*, 2017, p. 532 ; F. Rouvière, « La justice prédictive, version moderne de la boule de cristal », *RTD. civ.*, 2017, p. 527 ; D. Mainguy, « Regard prédictif sur la justice prédictive », note du 14 mars 2017 sur daniel-mainguy.fr ; A. Garapon et J. Lassègue, *Justice digitale*, PUF, hors collection, 2018.

66. - J. Dupré, *loc. cit.*

67. - A. Garapon (art. préc.) rappelle cependant les ambitions affichées des *legal tech*, qui vont au-delà d'une puissance capacité d'induction-déduction, et visent à apercevoir derrière le brouillard des données les « règles des règles » qui expliquent le fonctionnement du droit : « [...] les legaltech opèrent un saut qualitatif majeur. S'ils ne touchent pas à la règle primaire, ces logiciels formalisent non seulement les règles d'application de la règle, mais ils permettent de prévoir le traitement réservé par l'institution à des cas particuliers. Les big data prétendent conférer en effet une consistance non pas juridique, mais mathématique à une réalité que les juristes ne pouvaient atteindre que par un savoir intuitif et que la statistique approchait de manière trop générale ».

approuvant ou rejetant le projet de la machine, et à construire des raisonnements inédits lorsque la nouveauté de la situation mettra la logique informatique en échec.

17. Prophéties auto-réalisatrices - En revanche, il est plus difficile de savoir si l'on pourra se débarrasser un jour de ce dernier maillon de l'actuelle chaîne humaine. Pour savoir si le métier de juriste peut être mis en équations, il faut répondre à la question, qui n'a jamais trouvé de réponse définitive, de ce qu'est le droit. S'il ne relève pas, au fond, de la pure logique formelle, alors il ne pourra jamais être parfaitement modélisé⁶⁸. Toutefois, il n'est pas exclu qu'il change subrepticement de nature une fois les indicateurs logiciels mis en place : c'est ce que M. Garapon qualifie de « risque de performativité »⁶⁹. En effet, le magistrat qui aura l'impression que la décision qu'il s'apprêtait à prendre va à l'encontre d'une tendance locale ou nationale écrasante va-t-il maintenir sans trembler son jugement ? Le risque est grand d'éradiquer les raisonnements minoritaires, y compris lorsqu'ils sont le fruit d'une pure apparence : peut-être le logiciel n'a-t-il présenté au rédacteur sa position de dissident qu'en vertu d'un rattachement intellectuellement faux du cas d'espèce à une catégorie à laquelle il ne devait pas appartenir. Le juge pourrait ne pas s'en apercevoir, et se plier à un paradoxe qui n'existe que dans l'algorithme, mais deviendrait peu à peu le droit véritable. Une boucle de rétroaction se met en effet en place : plus l'algorithme convainc qu'une décision va certainement être adoptée, plus elle est adoptée effectivement. La prophétie est autoréalisatrice. Et le juriste humain abdique peu à peu ses prérogatives, sans s'en apercevoir, intimidé par l'omniscience et l'infailibilité prétendues de la machine, qui de mythes deviendront jour après jour réalité. Menons cet exercice de pensée jusqu'à son terme : l'autorité de l'algorithme est devenue incontestable, l'assistant est devenu le maître, la prédiction vaut certitude. Le professionnel du droit n'est plus nécessaire ; il n'est en tout cas plus utile. Ce déplaisant scénario, pour qui croit à l'incompressible part d'humanité du droit, n'a que fort peu de chances de se produire - gageons-le.

68. - F. Rouvière, art. préc. : « D'abord, est-on parfaitement certain que le droit relève du modèle de la causalité ? En effet, la prédiction suppose une forme minimale de déterminisme où les mêmes causes produisent les mêmes effets. Nous ne nions pas le fait que le droit soit influencé par des facteurs divers (sociaux, moraux, politiques, idéologiques, etc.). Cependant, l'argumentation juridique est une logique de justification. Les arguments n'expliquent pas la décision du juge, ils la justifient ». D. Mainguy, art. préc. : « La justice, la fonction de juger, est une affaire d'interprétation, dont la description est d'ailleurs si difficile qu'il faut des ouvrages très complexes et très disputés (V. H. Kelsen, M. Troper, B. Frydman, etc.), c'est-à-dire des trésors d'intelligence et d'expérience pour simplement tenter de parvenir à s'entendre sur les termes du débat de ce qu'est une interprétation juridique ».

69. - A. Garapon, art. préc. : « Un juge peu courageux est tenté d'estimer que si la majorité de ses collègues tranche dans ce sens, le moins dangereux pour lui est de les suivre. C'est l'effet "moutonnier" de la justice prédictive qui pousse au conformisme et réclame plus aux juges qui estiment qu'ils doivent aller à contre-courant, c'est-à-dire qui veulent faire leur métier tout simplement ! Cela sera également plus difficile pour les avocats plaidant des solutions alternatives, ou voulant faire changer une jurisprudence ».

Sans doute les intelligences numériques ne jouiront-elles jamais d'une parfaite autonomie d'action dans les métiers du conseil juridique ni dans le déroulement du procès. Mais il est des situations dans lesquelles elles peuvent d'ores et déjà agir sans entrave.

3 - Les actions automatisées

18. Un bras armé du droit ? - La fonction du système juridique qui consiste à s'assurer que les normes édictées sont effectivement mises en œuvre est parfois dévolue à des technologies numériques. Il ne s'agit plus seulement, alors, de préparer l'intervention des professionnels du droit, mais, dans une certaine mesure, de s'y substituer.

En effet, il arrive aujourd'hui que des dispositifs numériques soient mis en place pour contraindre leurs utilisateurs au respect de normes, qui sont en apparence d'origine légale ou contractuelle. Ainsi, il est fréquent que des supports d'œuvres de l'esprit, ou des machines destinées à lire ces supports soient les réceptacles de « mesures techniques de protection » (MTP). Elles empêcheront par exemple que soit copié un DVD, ou qu'un jeu vidéo n'ayant pas fait l'objet d'une acquisition légale puisse être lancé sur une console. Ces MTP se présentent ainsi *prima facie* comme des sentinelles numériques du droit de la propriété littéraire et artistique. Nous aurons l'occasion de les étudier en détail⁷⁰. La réalité apparaîtra alors bien plus nuancée : il se rencontre des protections techniques empêchant que soient copiés puis collés des extraits d'une œuvre appartenant au domaine public, ou interdisant qu'une vidéo soit mise en ligne, si elle contient des extraits d'un film protégé, alors même qu'il s'agit d'une parodie autorisée par la loi⁷¹. Ce n'est donc pas le droit qu'elles appliquent, mais un ensemble de règles qui peut s'en rapprocher jusqu'à la concordance, ou s'en éloigner jusqu'à la trahison.

Les *smart contracts* en constituent un autre exemple. Il s'agit de dispositifs informatiques auxquels a été enseignée une « règle du jeu » qui appellera des sanctions automatisées. Ils peuvent fort bien incorporer un véritable contrat juridiquement obligatoire, et lui prêter leur force : ainsi d'un contrat d'assurance qui stipulerait qu'après dix heures de gel consécutives lors d'une certaine période de l'année, une indemnité d'un certain montant doit être virée à un assuré vigneron, qui aura nécessairement perdu sa récolte. Connecté à des services de météorologie en amont, et à des instruments de paiement en aval, l'automatisme peut réaliser seul que les conditions du sinistre sont réunies et procéder au règlement nécessaire, sans intervention humaine. L'éviction de l'homme du processus serait, là encore, un gage d'efficacité : la machine serait impitoyable, mais juste. Dure est

70. - Sur lesquelles V.infra, n° 230 s.

71. - Ce dernier exemple est développé infra, n°234.

la loi numérique... mais est-elle la loi ? De même qu’avec les MTP, il faut observer que les sentinelles techniques peuvent incidemment se contenter d’une mise en œuvre des règles du système juridique classique. Mais elles peuvent également recevoir des instructions qui ne correspondent à aucune loi, à aucun contrat, ou à un contrat illégal - par exemple, vicié de violence sans qu’elles soient en mesure d’en tenir aucun compte.

De la collaboration à la concurrence avec le droit, il n’y a qu’un pas, que les technologies numériques sont susceptibles de franchir, puisqu’elles véhiculent leurs propres règles.

B - Les rapports de concurrence

19. La normativité numérique : l’exemple du jeu vidéo - Dans son ouvrage *Code and other laws of cyberspace* — devenu *Code V2* dans sa deuxième édition -, le constitutionnaliste américain Lawrence Lessig s’intéresse au fonctionnement du jeu vidéo en ligne *Second Life*, grand succès des années 2000 qui fonctionne toujours à bas bruit⁷². Le titre de l’œuvre traduit son ambition démiurgique : celle d’offrir au joueur une vie supplémentaire, par l’intermédiaire d’un avatar qui évoluera dans un univers virtuel peuplé de milliers d’internautes. Chacun est libre de s’y faire touriste, mendiant, poète, guerrier, anarchiste, prostitué. La monnaie qui a cours dans le jeu, le dollar Linden, peut être convertie en argent réel : certains joueurs s’assurent ainsi quelques revenus, voire de véritables moyens de subsistance, par exemple en vendant des représentations numériques d’œuvres d’art dont ils sont les auteurs, qui orneront les murs pixelisés de résidences fictives. Bien sûr, le droit de la liberté d’expression ou celui de la propriété intellectuelle ont vocation à s’appliquer aux activités menées dans *Second Life*, mais ce n’est pas l’enjeu de la démonstration de M. Lessig. Il relate une dispute à laquelle il a assisté au sein du jeu. Sur le terrain appartenant à une joueuse, Martha, poussaient des fleurs magnifiques aux pétales empoisonnés. Elle en faisait commerce auprès d’internautes sensibles à cette singulière rencontre entre la beauté et la mort. Un jour, le chien d’un autre joueur, Dank, avala un pétale et mourut après avoir beaucoup souffert. Dank tenta de convaincre Martha de reprogrammer ses fleurs pour qu’elles soient non létales ; Martha rétorqua que Dank pouvait reprogrammer son chien pour le rendre immortel. Ils s’accordèrent finalement sur une solution plus subtile.

“Okay,” said Dank, “why not make the petals poisonous only when in the possession of someone who has ‘purchased’ them? If they are stolen, or if they blow away, then let the petals lose their poison. But when kept by the owner of the plant, the petals keep their poison. Isn’t that a solution to the problem that both of us face?” The idea was ingenious. Not only did it help Dank, it helped Martha as well. As the code existed, it

72. - L. Lessig, *Code V2*, op. cit., p. 10 s. Pour un aperçu de cet univers, V. par ex. M. Tual, « Absurde, créatif et débauché : dix ans après, “Second Life” est toujours bien vivant », article *lemonde.fr/pixels* du 28 avril 2016.

allowed theft [...]. But if Martha could modify the code slightly so that theft removed a plant's poison, then "theft" would also remove the plant's value. That change would protect the profit in her plants as well as protect Dank's dogs. Here was a solution that made both neighbors better off—what economists call a pareto superior move. And it was a solution that was as possible as any other. All it required was a change of code⁷³.

L'exemple du jeu vidéo n'a pas été choisi au hasard. Au-delà de son aspect divertissant, il constitue une manifestation paroxystique — et d'autant plus facile à apercevoir — d'une vérité générale : le monde numérique est un agglomérat de règles. Chacun sait que le personnage de Mario grandit lorsqu'il entre au contact d'un champignon, qu'il meurt lorsqu'il tombe dans un précipice, qu'il ne peut passer à travers un mur sauf, par exception, s'il s'agit d'un passage secret. Puisque l'univers du plombier moustachu ou celui de *Second Life* se présentent comme des métaphores ou des parodies de l'univers réel, le code informatique se donne à voir, avec une particulière clarté, comme une force normative. Dans ces mondes en miniature, il est « loi » comme le sont, dans le nôtre, les lois de la physique ou les lois des hommes.

Au premier abord, comme les lois de la physique, cette norme a pour propriété d'être auto-exécutante, en restreignant d'emblée l'univers des possibles. Mille fois, le joueur pourra précipiter Mario contre la même paroi. Si le développeur a décidé qu'il était interdit de la traverser, cela ne signifie pas seulement qu'une éventuelle infraction pourrait être détectée par une autorité, puis faire l'objet d'une punition. Non : on ne pourra tout simplement pas passer. Mais l'affirmation mérite aussitôt d'être relativisée : contrairement aux lois de la physique, mais à l'instar de toute règle de création humaine, la norme informatique est faillible. Un « bug » peut se produire : le code sera fidèlement exécuté par la machine, mais les buts que s'était fixés le concepteur ne seront pas atteints, parce qu'il aura commis une erreur. Cet échec pourra se produire accidentellement, ou être volontairement provoqué par un utilisateur, qui aura découvert l'existence d'une faiblesse et voudra l'exploiter.

Si le code peut être analysé à la lumière des intentions qui avaient animé son créateur, cela signifie qu'il est susceptible d'interprétation, ce qui accentue son cousinage avec les autres normes sociales. Il ne s'agit pas d'une interprétation par l'ordinateur : deux machines différentes devraient exécuter de manière strictement identique un même jeu d'instructions - le mot n'est pas anodin. Mais des discussions peuvent naître entre humains, concepteurs ou utilisateurs de la norme, visant à déterminer si le résultat obtenu est bien conforme à l'objectif initial. Une vieille plaisanterie de programmeurs l'illustre : « *this isn't a bug, but an undocumented feature* »⁷⁴. La différence entre le

73. - L. Lessig, *op. cit.*, p. 14.

74. - « Ce n'est pas un bug, c'est une fonctionnalité non documentée ». Pour un exemple remontant à 1984 :

bug et la fonctionnalité d'un programme tient parfois seulement au caractère involontaire du premier.

Le monde du *speedrun* illustre cette aptitude du code informatique à constituer un support d'interprétation. Les *speedrunners* sont des compétiteurs qui cherchent à atteindre la fin d'un jeu donné en un minimum de temps. Certains ne se contentent pas de jouer le mieux possible, manette en main : ils utilisent un ensemble de logiciels externes permettant de ralentir le temps, ou encore de revenir en arrière à volonté jusqu'à obtenir une séquence de jeu parfaite : cette méthode est dite *tool-assisted*. Est-ce un usage loyal du programme ? Pour la machine, il s'agit comme d'habitude de transcrire des signaux entrants en signaux sortants, à l'aide d'un logiciel en lui-même inchangé. Pourtant, un humain interrogé y verrait certainement une « triche ». D'autres cercles de compétiteurs exploitent le même jeu sans l'assistance d'aucun logiciel, mais en s'autorisant le recours à certains bugs⁷⁵. D'autres refusent toute exploitation de bug, mais sont amenés à définir cette notion : la volonté réelle ou supposée du programmeur est alors invoquée, comme on s'en rapporterait aux travaux parlementaires pour la loi⁷⁶. Ainsi, ces communautés partent d'un seul et même code informatique pour aboutir, par superposition d'interprétations fondamentalement différentes, à des comportements autorisés ou proscrits au joueur, d'une très grande variété.

20. « **Code is law** » - L'univers numérique est une mosaïque de règles. Les créatures de Turing sont des machines à obéir à un ensemble d'instructions mathématiques, des plus simples aux plus complexes. Il peut s'agir d'un simple algorithme visant à classer par ordre croissant une série de chiffres entrés par l'utilisateur sur son clavier. Des millions de lignes de code supplémentaires, et l'on obtient de véritables univers normatifs, dans lesquels sont enchâssés des choix politiques - au sens le plus large - affichés ou occultes, anodins ou fondamentaux. Un grand réseau social permettra à ses utilisateurs de « lever le pouce » face à un contenu, mais pas de le baisser⁷⁷. Un célèbre fabricant imposera aux acheteurs de ses téléphones d'utiliser exclusivement son magasin

http://groups.google.com/forum/?hl=en#!original/net.bugs.uucp/8-6IxzIxeZQ/2oKU6_gX9kwJ. Définition proposée par urbandictionary.com : « *Excuse made by software developers when they try to convince the user that a flaw in their program is actually what it's supposed to be doing* ». Le dialogue suivant est proposé à titre d'illustration : « *User: When I am on the item detail screen and click on "delete this item", the program returns to the item overview screen and the item is still there. Developer: Your access permissions don't allow you to delete items. It's not a bug, it's a feature* ».

75. - V. par ex. la liste très précise des techniques autorisées et de celles qui sont interdites pour le jeu *Zelda ocarina of time* sur <http://zeldaspeedruns.com/leaderboards/ooc/glitchless/rules>.

76. - A propos du jeu *Undertale*, un premier joueur demande s'il est autorisé, dans un *speed-run glitchless* (sans recours à aucun bug), de redémarrer le jeu pendant un dialogue particulièrement long afin de sauter cette phase et d'économiser ainsi de longues minutes. Un second joueur lui répond : « *Reloading the game isn't a glitch, after all. 'Glitchless' simply means "Don't exploit errors in the game code that Toby [Fox, le créateur du jeu] did not intend", essentially* » : <https://www.speedrun.com/undertale/thread/a38w8>.

77. - L'exemple est proposé par le magazine BiTS de la chaîne Arte dans son épisode « Code is law ».

d'applications, d'où il pourra bannir les produits de ses concurrents ou imposer sa vision de ce qu'est un contenu « décent »⁷⁸. L'encyclopédie Wikipédia s'offrira à la lecture, mais aussi à la modification de tout intéressé. Derrière les choix techniques, ces exemples révèlent sans grand détour des prises de position implicites sur des valeurs sociales. De tels arbitrages sont parfois plus subtils, plus discrets ; ils n'en sont pas moins omniprésents. La plupart des acheteurs de musique dématérialisée ne se sont pas encore posé la question de savoir s'ils pourraient léguer leur vaste « audiothèque » à leurs enfants, comme on laissait derrière soi une malle de vieux vinyles. L'interface de la plateforme ne le permet pas, et cette plate évidence prévient à elle seule le débat. Mais derrière l'absence d'un bouton ou d'un menu permettant d'envisager ce legs, dans le creux, par-delà le vide, c'est une certaine conception du patrimoine numérique, de la propriété des objets incorporels, de la distinction entre biens et services, qui se révèle. C'est une règle qui s'applique, dont les concepteurs sont mal identifiés, adoptée au terme d'un processus souterrain.

C'est tout le sens de la formule-choc imaginée par M. Lessig : « Code is law ». Elle a parfois été décrite comme « une règle libertaire », un cri d'allégeance exclusive à la norme informatique, instituée seule loi véritable⁷⁹. Le contresens est frappant : son auteur l'avait conçue, bien au contraire, comme une mise en garde. Le fait qu'il existe une *lex informatica* est un simple constat, axiologiquement neutre⁸⁰. Mais la société en général, et les juristes en particulier, doit ensuite être attentive à la manière dont ces puissants leviers sont actionnés.

Code will be a central tool in this analysis. It will present the greatest threat to both liberal and libertarian ideals, as well as their greatest promise. We can build, or architect, or code cyberspace to protect values that we believe are fundamental. Or we can build, or architect, or code cyberspace to allow those values to disappear. There is no middle ground. There is no choice that does not include some kind of building. Code is never found; it is only ever made, and only ever made by us. As Mark Stefik puts it, "Different versions of [cyberspace] support different kinds of dreams [...]"⁸¹.

78. - V.infra, n°257.

79. - « Code is law » est qualifié de « règle libertaire », par ex., par P. Pailler, « L'intermédiation en question. L'apport des FinTechs au droit bancaire », *RDBF*, n° 2, mars 2017, dossier 12. Rapp., D. Legeais, « Blockchain », fasc. 534 in *J.-Cl. commercial*, mars 2017, n°15, qui estime que « les promoteurs d'Internet avaient initié ce slogan. Autrement dit, les participants se forgent leurs propres règles ». De manière générale, d'après ces auteurs, cette acception dévoyée de la formule se serait développée dans le milieu des blockchains.

80. - L'expression « lex informatica » est de J. R. Reidenberg, « Lex informatica : the formulation of information policy rules through technology », *Texas Law Review*, n° 76, 553 (1997-1998). Disponible sur : http://ir.lawnet.fordham.edu/faculty_scholarship/42

81. - L. Lessig, *Code V2*, op. cit., p. 6. La citation intercalée est de Mark Stefik, "Epilogue: Choices and Dreams," in *Internet Dreams: Archetypes, Myths, and Metaphors*, Cambridge, Mass.: MIT Press, 1996, 390. L'article intitulé « Code is Law » (*Harvard magazine*, janvier 2000) constitue un (trop) bref résumé des thèses développées dans *Code and other laws of cyberspace*, devenu *Code V2*.

Le droit entretient bien évidemment des relations — de soutien mutuel, d'affrontement, d'indifférence réciproque — avec d'autres systèmes normatifs, parmi lesquels on compte les règles morales, religieuses ou même sportives. Mais celles-ci sont directement perçues, et se présentent ouvertement comme des systèmes de régulation des comportements humains. L'influence de la *lex informatica*, quant à elle, est plus subreptice. Elle se niche et se cache au sein de créations techniques. On ne voit pas d'exemple, hors du numérique, d'objets susceptibles d'emporter avec eux des ensembles complexes de règles, tapis dans l'ombre. Évidemment, un cadenas fermé est un moyen de réguler les comportements au moyen d'une règle simple : passe celui qui dispose de la clé. Le verrou peut, ce faisant, renforcer ou défier le droit de propriété, ou celui d'aller et venir, selon qui l'a placé, et où. Bien sûr, une voiture peut être conçue, sans même embarquer de logiciel, pour avoir ou non la puissance nécessaire à un net dépassement de la vitesse maximale sur autoroute. Ces exemples n'approchent pas, de très loin, celui d'un livre numérique qui peut dicter à son utilisateur le temps de lecture quotidien dont il dispose, ou s'il est autorisé à revenir en arrière et sur combien de pages, ou s'il lui est permis d'obtenir une sortie papier du texte sur une imprimante⁸². Ils ne peuvent pas non plus être comparés aux routeurs d'un fournisseur d'accès à Internet, capables d'analyser les informations envoyées par un abonné sur le réseau et d'interdire la téléphonie sur IP, de ralentir le service de vidéo à la demande d'un concurrent et de rendre prioritaire la circulation des contenus d'une société amie⁸³.

Le numérique est ainsi constitué d'une myriade de systèmes normatifs embarqués, dans des objets incorporels ou corporels, dans des systèmes d'exploitation ou des logiciels d'applications, dans des puces, dans des réseaux de communication, des protocoles. De surcroît, le code informatique est souvent inconnu dans ses détails. Lorsqu'il se retrouve en compétition avec les règles de la morale ou d'une religion, le système juridique en connaît non seulement les effets, mais encore les principes. Le code informatique est régulièrement enfermé dans une « boîte noire » : l'observateur sait seulement ce qui y entre et ce qui en sort. Moyennant compétence et observations, il peut seulement tenter de deviner de son mieux ce que l'on dérobe à son regard.

Le défi lancé au système juridique est considérable. Mais il doit être relevé.

82. - V.infra, n°233.

83. - La téléphonie sur IP consiste à faire transiter la voix non pas directement par le réseau téléphonique classique, mais en tant que données circulant sur internet. Les modes de facturation distincts rendent souvent la voix sur IP plus intéressante pour des communications internationales, ce qui lui attire l'hostilité des opérateurs téléphoniques. Sur la neutralité du réseau en général, V.infra, n°185.

C - Les rapports de soumission

21. Intérêt d'une approche globale - Depuis les années 60, les technologies numériques ont vu leur importance croître de manière exponentielle. L'affirmation se vérifie tant sur le plan économique, où elles sont regardées comme un facteur de production, que sur celui de la culture, des loisirs, des mœurs. Outil de travail et de divertissement, instrument de projection vers le monde ou de repli vers l'intime, le numérique s'est installé dans tous les compartiments de la vie sociale. Il y déploie sa normativité discrète et puissante. Le « code » prend à chaque instant de nouveaux décrets, prononce des jugements sans appel et promulgue une loi silencieuse. Le système juridique n'est pas forcé de lui donner perpétuellement la réplique, et d'épuiser ses forces dans une perpétuelle logorrhée. Grâce au doyen Carbonnier, on sait que le silence de la loi doit être présumé choix plutôt que lacune : le non-droit est encore du droit⁸⁴. Mais qu'il agisse ou qu'il se taise, le législateur doit décider et non subir. Pour éclairer ses choix, les valeurs sociales mises en jeu par le numérique doivent être placées en pleine lumière, présentées et débattues. Des réactions appropriées pour le système juridique devraient alors être proposées, qu'il s'agisse d'encourager, de réprimer ou d'ignorer. Lorsque ces réactions ont déjà eu lieu, ce qui sera fréquent, il faudrait en évaluer les résultats.

L'entreprise est vaste. Bien des ouvrages y ont déjà concouru. Mais les manuels de droit du numérique ont pour objectif principal de délivrer un exposé clair, détaillé et technique des règles de droit positif ; s'ils ne se privent pas de développements théoriques et prospectifs, s'ils ne s'interdisent pas d'évoquer des problèmes encore non ou mal résolus, telle n'est pas leur vocation première⁸⁵. En revanche, les thèses de doctorat peuvent et doivent s'affranchir des limites de l'existant. Mais puisqu'elles visent une parfaite exhaustivité, elles sont nécessairement cantonnées à des problèmes bien circonscrits, et peuvent difficilement hausser leur niveau de généralité au-delà de la confrontation du numérique et d'une discipline entière du droit privé⁸⁶. Il paraît donc exister un espace pour une recherche qui soit à la fois principalement théorique et prospective dans son approche, et vaste dans son étendue.

84. - J. Carbonnier, *Flexible droit, pour une sociologie du droit sans rigueur*, LGDJ, 10e édition, 2001, première partie : « Droit et non-droit ».

85. - Parmi les ouvrages d'exposé du droit positif explicitement consacrés au numérique ou à une notion très voisine : H. Bitan, *Droit et expertise du numérique. Créations immatérielles, données personnelles, e-réputation, droit à l'oubli, neutralité, responsabilités civile et pénale*, Lamy, coll. Axe droit, 2015 ; C. Castets-Renard, *Droit de l'Internet. Droit français et européen*, Montchrestien-Lextenso, 2e éd., 2012 ; C. Féral-Schuhl, *Cyberdroit. Le droit à l'épreuve de l'Internet*, Dalloz, 6e éd., 2010 ; P. Gaudrat et F. Sardain, *Traité de droit civil du numérique, t. 1, Droit des biens*, Larcier, 2015 ; t.2, *Droit des obligations*, 2015 ; L. Grynbaum, C. Le Goffic et L. Morlet-Haïdara, *Droit des activités numériques*, Dalloz, 2014 ; M. Vivant (ss. la dir.), *Lamy droit du numérique*, 2017.

86. - Elles seront citées au fil de l'étude.

22. Grandes notions du droit privé - Admettons qu'une telle étude présente quelque intérêt dans son principe, resterait à fixer la méthode. Comment faut-il approcher le vaste continent des relations entre droit et numérique ? La démarche la plus évidente consisterait à placer au premier plan des concepts intimement liés au monde des nouvelles technologies. Il pourrait s'agir d'objets relativement précis, comme les « réseaux sociaux », les « échanges de pair-à-pair », les « plateformes », ou « les liens hypertextes », ou bien de notions plus vastes, comme celle de « dématérialisation ». Chacun des sujets ainsi définis serait ensuite placé au contact des diverses disciplines du droit privé, afin que surgissent les difficultés à résoudre. Passer la création d'un lien hypertexte au crible du droit mobilisera aussi bien la matière pénale — si le contenu cible est diffamatoire, par exemple — que le droit de la propriété intellectuelle - si la page visée contient une œuvre protégée par le droit d'auteur.

C'est une démarche exactement inverse que nous nous proposons d'adopter. Doivent être placés au premier rang de l'analyse les concepts juridiques les plus classiques, les moins propres au numérique, les plus transversaux possible. Il ne s'agit en aucun cas de nier les spécificités de l'objet d'étude. Mais adopter pour point de départ les notions structurantes du droit privé évite de céder trop vite aux sirènes du *sui generis*. Nous tenterons de manipuler les questions nouvelles à l'aide d'outils anciens. En cas de succès, l'objet numérique se trouvera rattaché aux concepts communs comme la branche au tronc et sera, par là même, irrigué de la sève de réflexions séculaires. Si toutefois l'on échoue à appliquer l'instrument classique au problème nouveau, ce sera peut-être le signe que le concept doit être assoupli, précisé ou transformé : cela permet encore de relier le numérique aux acquis du droit privé, et peut simultanément offrir aux disciplines plus anciennes le bénéfice d'un instrument juridique rendu meilleur. Enfin, si et seulement si la notion classique est absolument inapte à saisir la difficulté qui lui est proposée, même au prix d'une évolution, la rupture devra être constatée avec le droit commun, et un corps de règles spécifiques devra être forgé. Cette dernière solution ne peut pas être rejetée par principe, mais doit toujours conserver un caractère subsidiaire.

Afin d'éviter tout malentendu, précisons que nous ne considérons pas les grandes notions du droit privé comme figées, toujours égales à elles-mêmes à travers le temps. S'adaptant sans cesse aux évolutions de la société humaine, elles sont en mouvement constant. Le numérique aura-t-il une influence, marginale ou substantielle, sur leur trajectoire ? C'est ce qu'il nous faut déterminer.

Si l'on se réfère à la liste des grandes notions du droit privé récemment proposée par Madame Rochfeld, il est évident que leur confrontation systématique avec l'univers numérique nécessitera de

longues années d'analyse⁸⁷. Tout en nous fixant ce programme pour l'avenir, nous en présentons ici une entame — substantielle — en vue de l'habilitation à diriger des recherches. Elle porte sur trois concepts classiques, dont il sera démontré qu'ils entrent en résonance, de manière particulièrement puissante, avec l'univers numérique : la personne (première notion), la propriété (deuxième notion) et le contrat (troisième notion).

87. - J. Rochfeld, *Les grandes notions du droit privé*, PUF, Thémis droit, 2ème éd., 2013. L'auteur envisage tour à tour la personne, les groupes de personnes, les droits subjectifs, le bien, la propriété, le patrimoine, le contrat et la responsabilité.

Première notion - La personne

23. **La clé de voûte du droit privé** – « La personne, au sens de l'individu, a été conçue comme la notion centrale du droit »¹. Les droits réel en général et la propriété en particulier, les contrats, la responsabilité civile ou pénale ne prennent leur sens qu'à travers elle et pour elle. Ils sont en quelque sorte des notions secondes, qui n'existent que pour animer et enrichir les relations interpersonnelles. Pour le *Vocabulaire juridique*, d'ailleurs, la « personne » est d'abord « celui ou celle qui jouit de la personnalité juridique », c'est-à-dire de « l'aptitude à être titulaire de droits et assujetti à des obligations [...] »². Le droit gravite autour de l'individu.

D'un point de vue étymologique, le mot « personne » renverrait au latin « *persona* », qui désigne le masque de théâtre³. Lui-même serait issu de « *per sonare* », « ce par l'intermédiaire de quoi le son se manifeste »⁴. Entre les traits véritables de l'acteur et le regard du public, le masque s'interpose. Il occulte une réalité et en impose une autre. Et en effet, à travers la notion de « personne », ce n'est pas la réalité profonde de l'être humain que l'on cherche à saisir, mais seulement sa projection publique. Le droit ne se mêle pas de la vie intérieure, mais il s'impose dans l'existence sociale.

Précisons qu'il ne sera guère question, ici, des regroupements de personnes physiques, c'est-à-dire des personnes morales. Associations et sociétés sont vivement confrontées au numérique dans le déroulement de leurs activités, mais les nouvelles technologies de l'information ne semblent remettre en question ni leur existence, ni les principes cardinaux qui les gouvernent.

En revanche, certaines règles essentielles qui touchent aux personnes humaines pourraient être atteintes.

24. **Numérique et frontières de la personnalité** – C'est l'une des questions les plus vertigineuses qui se rencontrent à la croisée de la philosophie du droit et du droit civil : à qui la qualité de personne doit-elle être reconnue ? Elle a pu être refusée, à travers le monde et l'histoire, aux esclaves, aux morts civils, aux membres de certaines ethnies ou aux adeptes de certaines

1. - J. Rochfeld, *Les grandes notions...*, op. cit., n° 1.1.

2. - G. Cornu (dir.), *Vocabulaire juridique de l'Association Henri Capitant*, 11e éd., 2016, V° « Personne » et « Personnalité juridique ».

3. - Ibid.

4. - F. Terré et D. Fenouillet, *Droit civil. Les personnes. Personnalité, incapacité, protection*, Dalloz, 8e éd., 2012, n° 10.

religions⁵. Aujourd'hui, dans notre pays, la recherche de limites internes à l'espèce humaine s'est cantonnée aux extrémités du fil de la vie : le fœtus et la dépouille mortelle sont des choses⁶.

À l'extérieur de l'espèce humaine, en revanche, les débats sont vifs pour savoir s'il conviendrait de reconnaître l'animal comme une personne. Il a jusqu'ici échoué à quitter le monde des choses, une réforme récente s'étant contentée de répéter qu'il est un bien à statut particulier — ce que nul n'ignorait — en tant qu'il est « doué de sensibilité »⁷. Certains, à l'instar de M. Marguénaud, plaident pourtant pour leur attribuer une personnalité, en précisant bien que cela n'impliquait pas nécessairement d'en faire les égaux des êtres humains :

Certains des attributs de la personnalité juridique de l'homme sont [...] trop somptueux pour l'animal qui ne saurait en retirer une quelconque utilité même avec la plus grande ingéniosité de celui qui le représenterait sur la scène juridique pour surmonter son incapacité à exercer les droits dont il pourrait avoir la jouissance. Activement, il serait donc déplacé de l'assimiler à la personne humaine. Il serait plus absurde encore d'essayer de lui faire supporter les obligations auxquelles la personnalité juridique expose l'être humain⁸.

Il se serait agi de leur reconnaître une « personnalité technique », de portée limitée, reposant sur un double constat : l'existence d'un intérêt distinct de celui des humains, et la possibilité d'être représenté – par leur « maître » ou une association de protection de la cause animale⁹.

Mais une deuxième figure est en train de surgir, dont on se demande si elle pourrait s'élever un jour à la dignité de personne. Elle est issue du monde numérique : il s'agit du robot. Encore faut-il préciser le propos. Un dictionnaire usuel définit le robot comme un « appareil automatique capable de manipuler des objets ou d'exécuter des opérations selon un programme fixe, modifiable ou adaptable »¹⁰. La plupart des membres actuels de cette vaste famille ne présentent aucune caractéristique qui justifierait d'ouvrir un débat sur leur personnalité. Ni l'appareil industriel destiné

5. - J. Rochfeld, *Les grandes notions...*, op. cit., n° 1.2.

6. - V. par ex. P. Malinvaud, *Introduction à l'étude du droit*, Lexisnexis, 14e éd., 2013, n° 274 s.

7. - Art. 515-14 C. civ., issu de la loi n° 2015-177 du 16 février 2015 relative à la modernisation et à la simplification du droit et des procédures dans les domaines de la justice et des affaires intérieures : « Les animaux sont des êtres vivants doués de sensibilité. Sous réserve des lois qui les protègent, les animaux sont soumis au régime des biens ».

8. - J.-P. Marguénaud, « La personnalité juridique des animaux », *D.*, 1998, 205.

9. - *Ibid.* Dire que ce type de propositions rencontre des résistances au sein de la doctrine est un euphémisme. Par exemple, F. Terré relève que la tendance « (...) à traiter l'animal quelque peu, voire beaucoup, à l'instar des personnes physiques » s'observe « (...) surtout dans les périodes de décadence [...] » (*Introduction générale au droit*, Dalloz, 9e éd., 2012, n° 227).

10. - *Dictionnaire Larousse en ligne*, V° « Robot ». L'ouvrage précise que le mot « [...] a été créé en 1920 par l'écrivain tchèque Karel Čapek, dans une de ses pièces de théâtre (R. U. R. [Rossum's Universal Robots]), pour dénommer un androïde construit par un savant et capable d'accomplir tous les travaux normalement exécutés par un homme ».

à peindre des automobiles à la chaîne, ni la machine domestique aidant à la confection des repas ne présentent de substance commune avec l'être humain. Si les animaux, ou une partie d'entre eux perceront peut-être un jour la muraille qui entoure la catégorie des personnes, c'est parce qu'ils ont en partage avec l'Homme une capacité à ressentir et à exprimer la joie comme la souffrance qui manque au règne végétal ; c'est parce qu'ils naissent, se reproduisent et meurent contrairement au règne minéral.

Pour savoir si les robots accéderont un jour à la personnalité, on peut donc s'interroger sur leurs points d'accroche à l'Humanité, qui sont autant de moyens d'émouvoir les maîtres du système juridique, et de raisons d'envisager cette mesure extraordinaire.

D'abord, certains robots feignent d'ores et déjà d'avoir une personnalité unique, et font mine de ressentir des émotions. Il ne s'agit pour l'heure que de subterfuges, mais qui sont propres à susciter l'empathie humaine. Pour se rendre plus attachants, ces robots prennent d'ailleurs la figure... de l'homme ou de l'animal. La presse s'est amusée ou effrayée de cet ingénieur chinois « épousant » un robot de sa conception, après avoir renoncé à rencontrer l'amour dans un pays où les hommes sont bien plus nombreux que les femmes¹¹. De manière moins anecdotique, l'usage de robots imitant des animaux domestiques se développe dans certaines maisons de retraite¹². Le principal enjeu juridique est ici la création d'un statut de bien particulier, apte à protéger la sensibilité de l'humain qui s'y est attaché. Le problème est facile à résoudre, puisqu'il se pose depuis longtemps avec de véritables chiens et chats : il s'agira d'admettre que la perte de ces objets peut être source d'un préjudice moral devant être réparé par un éventuel responsable, ou encore de statuer sur des problèmes de garde après la séparation d'un couple¹³. Jusqu'ici, pas l'ombre d'un droit n'apparaît dans le chef des robots : des hommes assignent leurs semblables, afin que prévalent des intérêts purement humains.

Ensuite, si l'on restreint le propos à cette catégorie particulière de robots qui vise à ressembler au maximum à l'humain, un problème se pose qui ne se rencontrait pas face à l'animal : faut-il reconnaître un statut particulier à la chose qui symbolise l'Homme ? La figure de l'androïde est ancienne dans la fiction. Dans *l'Illiade*, déjà, le dieu difforme Héphaïstos compense ses infirmités

11. - B. Haas, « Chinese man "marries" robot he built himself », article *theguardian.com* du 4 avril 2017.

12. - B. Britto, « Animatronic pets at retirement homes a sign of how robots will contribute to our lives », article *baltimoresun.com* du 30 mars 2017.

13. - C'est en 1962 que la Cour de cassation a jugé, dans un célèbre arrêt *Lunus*, « qu'indépendamment du préjudice matériel qu'elle entraîne, la mort d'un animal peut être pour son propriétaire la cause d'un préjudice d'ordre subjectif et affectif susceptible de donner lieu à réparation [...] » (Cass. 1ère civ., 16 janvier 1962 : Bull. civ., n° 33). Sur le problème de la garde de l'animal après une rupture, V. not. P. Hilt, « L'animal de compagnie lors de la séparation du couple », *AJ Famille*, 2012, p. 74.

par son génie technique, y compris en plaçant à son service des esclaves artificiels : « Il mit une tunique, prit un sceptre énorme et sortit de la forge en boitant. Et deux servantes soutenaient les pas du Roi. Elles étaient d'or, semblables aux vierges vivantes qui pensent et parlent, et que les Dieux ont instruites. Soutenu par elles et marchant à pas lourds, il vint s'asseoir auprès de Thétis, sur un trône brillant »¹⁴. Dans la fiction récente, cette fois-ci, la série télévisée *Westworld* a mis en scène des androïdes placés dans un parc d'attractions pour l'agrément des touristes¹⁵. Les visiteurs sont invités à les battre, les tuer ou les violer selon leur bon plaisir. Quand bien même ces créatures seraient inaptes à la souffrance physique ou morale, on peut se demander si réserver un tel sort à une représentation aussi réaliste de l'humain — un androïde est plus qu'une simple statue de marbre — n'est pas de nature à heurter des valeurs sociales importantes. Dans ce paradigme, les robots restent des choses et le droit n'est pas mis au défi. Le problème est redoutable d'un point de vue philosophie ou morale, mais il appelle des traductions techniques tout à fait maîtrisées. Des mesures de police administrative, prises sur le fondement de l'atteinte à la dignité humaine, voire l'adoption d'incriminations pénales spécifiques sont tout à fait envisageables.

Enfin, c'est un ordre de difficultés très différent qui s'ouvre si l'on postule que les créatures artificielles pourront un jour accéder à la conscience d'elles-mêmes – c'est le cas des servantes d'Héphaïstos comme des androïdes de *Westworld*. Ce moment est appelé « singularité » dans la littérature de science-fiction. Il est loin d'être certain qu'il se produira un jour dans la réalité¹⁶. Si cela advenait, alors bien évidemment la question de la personnalité juridique des robots se poserait, mais dans des termes qu'il est, par hypothèse, impossible d'anticiper. Pour l'heure, l'« intérêt distinct », qui fonde la proposition de M. Marguénaud relative à l'animal, n'existe pas. Il semble par conséquent prématuré d'évoquer, comme le fait une résolution du Parlement européen :

*(...) la création, à terme, d'une personnalité juridique spécifique aux robots, pour qu'au moins les robots autonomes les plus sophistiqués puissent être considérés comme des personnes électroniques responsables tenues de réparer tout dommage causé à un tiers; il serait envisageable de conférer la personnalité électronique à tout robot qui prend des décisions autonomes ou qui interagit de manière indépendante avec des tiers*¹⁷.

14. - Homère, *L'Iliade*, chant XVIII, trad. Leconte de Lisle (1866). Sur les robots d'Héphaïstos : T. Berthier, « La robotique et le temps du Kronos », article *humanoides.fr* du 29 juin 2016 ; A. Marcinkowski et J. Wilgaux, « Automates et créatures artificielles d'Héphaïstos : entre science et fiction », *Techniques et culture*, n° 43-44, 2004.

15. - J. Nolan et L. Joy, *Westworld* (2016). L'œuvre revisite une série du même nom datant de 1974, créée par M. Crichton et interprétée notamment par Y. Brynner.

16. - Certains doutent que cela puisse se produire, même à long terme : J.-G. Ganascia, *Le mythe de la singularité : faut-il craindre l'intelligence artificielle ?*, éd. Du Seuil, 2017.

17. - Parlement européen, Résolution du 16 février 2017 contenant des recommandations à la Commission concernant des règles de droit civil sur la robotique (2015/2103(INL)), point 59, f). Dans le même sens : A.

La proposition laisse perplexe, en ce qu'elle semble mélanger deux problèmes bien distincts. Que les dommages causés par les robots et intelligences artificielles appellent des réflexions en droit de la responsabilité civile, c'est une évidence. Ces difficultés se rattachent largement à la question, plus large, de la responsabilité du fait du fonctionnement des algorithmes. Mais c'est bien une personne physique ou morale classique qui devra assumer le paiement d'éventuels dommages-intérêts : la reconnaissance d'une personnalité au robot n'apporterait aucun progrès à cet égard¹⁸.

Une étude mêlant droit positif et prospective à court et moyen terme doit donc traiter essentiellement du « droit des robots » comme d'un problème de responsabilité civile. C'est sous cet angle qu'il sera abordé ultérieurement¹⁹.

25. Numérique et droits de la personnalité – À la question de savoir qui sont les personnes juridiques, les technologies numériques n'apportent donc pas, pour l'heure, de réponse inattendue. Mais lorsqu'il s'agit, en revanche, d'évoquer les droits attachés à la personnalité, leur influence est manifeste. L'histoire des droits de la personnalité est très récente. Des auteurs rappellent que les rédacteurs du Code civil ont « totalement ignoré » la question, comme le droit romain et l'ancien droit avant eux²⁰. « Le code civil a consacré 174 articles aux successions, 194 aux régimes matrimoniaux et 20 aux murs et fossés mitoyens ; mais la loi n'a rien dit ni sur les moyens de défendre le nom patronymique, ni sur les droits non patrimoniaux de l'auteur et de l'artiste... »²¹. La première consécration textuelle d'un droit de la personnalité date d'une loi du 17 juillet 1970²². C'est elle qui crée l'article 9 du Code civil, aujourd'hui célèbre et dont le premier alinéa dispose : « Chacun a droit au respect de sa vie privée ». Le législateur réagissait principalement à des progrès technologiques, permettant tout à la fois de s'immiscer dans la sphère intime des individus pour y dérober leurs secrets, et de diffuser largement le fruit de ces rapines²³. Or, le numérique a contribué

Bensoussan, « Droit des robots : science-fiction ou anticipation ? », *D.*, 2015, p. 1640.

18. - En ce sens : A. Mendoza-Caminade, « Le droit confronté à l'intelligence artificielle des robots : vers l'émergence de nouveaux concepts juridiques ? », *D.*, 2016, p. 445 ; A. Bensamoun, « Des robots et du droit... », *Dalloz IP/IT*, 2016, 281 ; Comité économique et social européen, *L'intelligence artificielle*, avis d'initiative du 31 mai 2017.

19. - Une prochaine version de l'étude consacrera « la responsabilité civile » au sein des notions de droit privé méritant d'être confrontées au numérique.

20. - J.-M. Bruguière et B. Gleize, *Droits de la personnalité*, éd. Ellipses, 2015, n° 1.

21. - R. Lindon, *Les droits de la personnalité*, Dalloz, 1974, n° 3, cité par J.-M. Bruguière et B. Gleize, loc. cit.

22. - Loi n° 70-643 du 17 juillet 1970 tendant à renforcer la garantie des droits individuels des citoyens.

23. - Sur les rapports entretenus par la « personnalité » et « l'identité » : J.-M. Bruguière et B. Gleize, *op. cit.*, n° 4.

à démultiplier ces menaces : ce n'est pas un hasard si la deuxième grande loi relative aux droits de la personnalité, datant de 1978, est celle relative à l'informatique et aux libertés²⁴.

La question est discutée de savoir s'il existe « un » ou « des » droit(s) de la personnalité ; si l'on défend séparément le nom, la vie privée, l'honneur, ou si plus fondamentalement il s'agit à chaque fois de défendre la personne²⁵. En matière de numérique au moins, il nous semble que ces différents combats peuvent être regroupés en un seul. Ce que la personne défend, c'est son « identité » : on retrouve le masque de théâtre qu'elle dirige vers le monde²⁶. Cette interface qui définit en même temps qu'elle protège, les forces de traitement numériques de l'information risquent de la défigurer, ou de la contourner pour accéder à une vérité sur l'individu qui devait demeurer cachée. L'identité numérique doit donc retenir notre attention.

26. Numérique et liberté d'information – Les droits de la personnalité ont une nature essentiellement défensive, ils s'analysent en un « droit de contrôle »²⁷. Mais s'intéresser à la personne, c'est aussi examiner des droits et libertés fondamentaux visant à sa construction et à son épanouissement. Parmi ceux-ci, il est évident que la liberté d'information a été profondément bouleversée par le numérique. L'article 10 de la Convention européenne des Droits de l'Homme dispose en effet que la liberté d'expression comprend non seulement la liberté d'opinion, mais encore « la liberté de recevoir ou de communiquer des informations ou des idées [...] ». Or, tel est précisément l'objet de la mise en réseau des intelligences numériques : la communication.

27. Plan – Nous décrirons donc le rôle d'Internet comme interface sociale, sous un jour tour à tour défensif et expressif. À l'examen de l'identité numérique (chapitre 1) succédera celui de la communication numérique (chapitre 2).

24. - Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

25. - V.infra, n°97.

26. - J.-M. Bruguière et B. Gleize, *op. cit.*, n° 28 :

27. - A. Lepage, « Personnalité (droits de la) », in *Répertoire civil Dalloz*, avril 2017, n° 11.

Chapitre 1 - L'identité numérique

28. L'identité comme essence - Dans un dictionnaire usuel, « l'identité » peut se définir comme « le caractère permanent et fondamental de quelqu'un, d'un groupe, qui fait son individualité, sa singularité »²⁸. Définir ce qui est au fondement d'un être : l'opération semble démesurément ambitieuse. Elle l'est. M. Daniel Gutmann expose que l'identité personnelle, pour la philosophie, est la réponse à la question : « jusqu'à quel point peut-on changer tout en demeurant la même personne ? »²⁹. Il rappelle les expériences de pensée proposées au cours des siècles et visant à déterminer quand un individu cesse d'être lui-même. Ainsi Locke imagine-t-il le transfert de l'âme d'un prince dans le corps d'un savetier, avant de s'interroger : avons-nous toujours affaire à la même personne³⁰ ? Plus de trois siècles après, on voit se profiler le jour où le fantasme de l'intellectuel se transformera en une question solennellement soumise à un comité d'éthique. Les chirurgiens ont déjà procédé à des greffes de visages, et envisagent de greffer bientôt des têtes humaines sur des corps morts³¹. Le courant transhumaniste rêve quant à lui de répliquer la mémoire et les processus cérébraux d'un être humain dans les circuits d'une machine, après sa mort... voire de son vivant. Dans ces exemples, où se trouve l'individu ? À cette vertigineuse question, la philosophie n'apportera sans doute aucune réponse définitive.

29. L'identité stable - Mais le droit est-il si ambitieux ? À quelles fins fait-il appel au concept d'identité ? M. Gutmann constate que « l'identité personnelle est à l'évidence la condition de possibilité même du droit »³². Locke est à nouveau convoqué, pour qui le concept de « personne » sert à « approprie[r] des actions, et le mérite ou le démérite de ces actions »³³. Dans une société composée d'une multitude d'individus, le droit doit veiller à toujours créditer ou débiter le bon compte, lorsqu'il s'agit d'imputer des droits, des dettes, des sanctions, des honneurs par lui consacrés. Rechercher l'identité, selon la définition usuelle précédemment citée, c'est traquer la

28. - Larousse en ligne, V° « Identité », sens n° 3.

29. - D. Gutmann, *Le sentiment d'identité. Etude de droit des personnes et de la famille*, LGDJ, 2000, n°3, citant S. Ferret, *Le philosophe et son scalpel. Le problème de l'identité personnelle*, éd. de Minuit, coll. « Propositions », 1993, p. 17.

30. - J. Locke, *Essai philosophique concernant l'entendement humain*, trad. P. Coste, Vrin, 1972, p. 269 s., cité par D. Gutmann, *Loc. cit.*

31. - C'est l'ambition de l'italien Sergio Canavero, à un horizon de quelques années : <http://www.rfi.fr/emission/20150308-grefe-cerveau-changer-corps>.

32. - D. Gutmann, *op. cit.*, n° 4.

33. - *Essai philosophique...*, *op. cit.*, II, 27, §26n p. 275, cité par D. Gutmann, *Loc. cit.*

singularité. Cela revient bien à caractériser un élément au sein d'un ensemble plus vaste, de sorte qu'on ne désigne que lui, et lui seul. Bien souvent, le droit pourra se contenter d'une identité resserrée, sèche mais efficace, qui ne vise pas à saisir l'individu dans toute sa complexité, mais simplement à l'isoler de ses contemporains, le temps par exemple de vérifier qu'il dispose d'un droit qu'il entend exercer, ou de lui imposer une contrainte. C'est « l'identité stable », qui renvoie à l'état des personnes et se compose par exemple du nom de l'individu, de sa date et de son lieu de naissance, de sa filiation³⁴. Elle vise à « l'identification de la personne dans le groupe social »³⁵ et constitue « une institution de police civile »³⁶. Les éléments les plus efficaces, dans cette entreprise d'identification, ne sont pas choisis par l'individu, mais lui sont donnés, et ne varient pas au cours de sa vie. Une façon commode de singulariser l'ensemble des citoyens français consiste à leur attribuer à chacun un identifiant unique. Il existe : c'est le numéro d'inscription au répertoire national d'identification des personnes physiques (ou NIR), souvent appelé « numéro de sécurité sociale »³⁷.

Entre la quête métaphysique du soi profond et la simple production du numéro de sécurité sociale, il semble évident que ce n'est plus la même « identité » que l'on recherche. Cela s'explique fort bien si l'on accepte l'idée que le droit fait un usage finalisé de cette notion. Il cherche à singulariser les individus dans une perspective précise.

30. L'identité choisie - Si l'identification des individus était la seule préoccupation du système juridique, l'utilisation du NIR dans les rapports administratifs et contractuels serait à la fois généralisée et suffisante. Cette suite de chiffres désigne aussi sûrement un citoyen parmi ses semblables qu'une longitude et une latitude désignent un et un seul point à la surface du globe. Mais la réduction des hommes à des matricules est de sinistre mémoire. Elle tend à couper l'individu tout à la fois de son passé et de son avenir.

Elle l'isole de son passé. Le nom et le prénom, même combinés, ont un pouvoir identifiant souvent insuffisant à eux seuls. Les cas d'homonymie doivent être repoussés par l'adjonction de la date et du lieu de naissance. Pourtant, ces informations sont couramment utilisées à des fins d'identification, parce qu'elles affirment une appartenance à un groupe familial, et inscrivent l'individu dans une continuité humaine, dans une histoire.

34. - J. Rochfeld, *Les grandes notions du droit privé*, op. cit., n° 1.16.

35. - *Ibid.*, n° 1.17.

36. - A.-M. Leroyer, « La notion d'état des personnes », in *Mélanges M. Gobert*, Economica, 2004, p. 253.

37. - <https://www.insee.fr/fr/metadonnees/definition/c1409>.

Elle l'isole de son avenir. À l'instant où l'individu naît, un NIR lui est attribué, qui ne variera plus jusqu'à son dernier souffle. Des informations telles que le domicile, la profession, sont en revanche susceptibles de changer rapidement. Leur efficacité comme instrument d'identification diminue d'autant, mais leur caractère sclérosant, enfermant, s'en trouve lui aussi amoindri. En s'identifiant par le jeu de telles informations, l'individu parvient à montrer qui il est — voire à le revendiquer, à s'affirmer — sans s'interdire de faire évoluer ces éléments caractéristiques à l'avenir, au gré de ses aspirations. Participent aujourd'hui de ce dynamisme des informations longtemps considérées comme immuables : le nom, et même l'appartenance à un genre. Comme l'explique un auteur, « La conception traditionnelle de l'identité juridique de la personne a évolué et continue aujourd'hui de se transformer. Le mouvement s'explique par l'influence de l'individualisme et des revendications de chacun de choisir les éléments de son identité juridique et de pouvoir les mettre en adéquation avec l'identité véritablement vécue » : c'est « l'identité choisie »³⁸.

31. L'identité comme représentation - Les individus chercheraient donc à reprendre le contrôle de leur identité. Si l'on prend ce dernier mot dans son sens philosophique, l'affirmation n'a guère de sens. Quel pouvoir a-t-on sur ce que l'on est profondément et essentiellement ? L'idée s'explique fort bien, en revanche, si l'on considère l'identité — ou l'une des acceptions de ce mot — comme une simple représentation de la personne, qui lui sert d'interface avec le monde social en général, et le monde du droit en particulier. M. Gutmann a ainsi consacré ses réflexions, non pas à « l'identité », selon lui insaisissable, mais plus modestement au « sentiment d'identité ».

*L'esprit a en effet naturellement tendance à se représenter, plutôt que des impressions successives et reliées entre elles, une identité (sameness). Cette illusion d'identité est le résultat d'opérations intellectuelles complexes, par lesquelles nous attribuons aux différents faits de l'expérience des propriétés de ressemblance, de contiguïté qui unifient et systématisent sa diversité. Pour Hume, la mémoire n'est donc pas ce qui nous permet de découvrir une quelconque identité personnelle, mais ce qui produit la croyance en son existence. De même, l'impression de permanence n'est-elle que le résultat de notre incapacité à nous rendre compte d'un changement lorsque celui-ci est proportionnellement infime*³⁹.

L'identité prise en ce sens est représentation. Une identité est un avatar de la personne, une construction, une vue de l'esprit. La vision que l'individu a de lui-même ne correspond pas nécessairement à la vision que la société et le droit ont de lui. Cette divergence peut l'affecter et il cherchera à la réduire, par exemple pour faire modifier son nom ou son genre à l'état civil. Cette divergence peut aussi lui être agréable : que la société ignore ou se représente inexactly une information le concernant protège son intimité.

38. - J. Rochfeld, *op. cit.* n° 1.18.

39. - D. Gutmann, *op. cit.*, n° 9.

L'identité, au sens où nous l'entendrons, est donc un ensemble d'informations qui prétendent décrire un individu à la société dont il est membre. Elles peuvent certes être employées pour identifier : afin de permettre au droit, l'espace d'un instant, d'isoler une brebis du troupeau pour qu'il soit procédé à une imputation, à son avantage ou à son détriment. Mais le droit ne peut s'en tenir là. Il doit donner à la personne les moyens de protéger cette interface sociale, ce « sentiment d'identité »⁴⁰, contre les agressions de toutes sortes. Certaines informations inexactes, déshonorantes, intimes, ne devraient pas circuler, prendre place dans l'avatar social.

32. L'identité numérique - Un « ensemble d'informations » ? Mais les technologies numériques ne sont rien d'autre que des vecteurs d'informations, d'une inégalable puissance. Dès lors, il est logique de se demander « [...] si, actuellement, les personnes ne sont pas en passe d'acquérir, superposée à leur identité sociale, une identité numérique composée des données à caractère personnel qu'elles disséminent sur Internet »⁴¹. La question est plus large encore, puisqu'un traitement numérique est appliqué à des données qui ne sont pas directement dévoilées sur Internet : un paiement par carte bancaire dans une boutique physique, laissant des traces dans les fichiers des banques et des commerçants, ou une déclaration fiscale sur papier, rapidement numérisée et intégrée aux fichiers de l'administration, en constituent deux exemples pris au hasard. Or, il semble difficile de distinguer deux avatars numériques dont l'un existerait « en ligne » et l'autre « hors-ligne », car toute information numérisée a aujourd'hui vocation à être intégrée à un réseau et, au moins potentiellement, à circuler.

Le réservoir d'informations numériques lié à chaque individu, on le devine, est gigantesque, y compris lorsqu'ils se connectent pas ou peu à Internet. Mais par ailleurs, si l'on considère à présent les seules activités en ligne, l'anonymat est souvent de rigueur, que ce soit sur les forums de discussion ou sur certains réseaux sociaux. Étrange univers, où l'on semble dire à la fois tout et rien de soi. L'avatar numérique est-il obèse ou translucide ?

Ce vaste ensemble d'informations peut servir deux fins parallèles : identifier l'individu auprès du système juridique d'autre part ; en donner une représentation sociale dirigée vers ses semblables d'autre part. C'est une tendance lourde du numérique que de brouiller les frontières entre ces deux fonctions traditionnelles de l'identité en droit.

Nous verrons quels sont les éléments constitutifs de l'identité numérique (section 1), puis comment cette identité est protégée par des moyens à la fois juridiques et techniques (section 2).

40. - D. Gutmann, *op. cit.*

41. - J. Rochfeld, *op. cit.*, n° 1.35.

Section 1 - Les éléments de l'identité numérique

33. **Identité stable, identité construite** - Mme Rochfeld estimait à juste titre que l'identité numérique se superpose aux formes d'identité plus anciennes, sociales et juridiques. Elle ne remplace pas l'existant. Au contraire, son noyau semble constitué des éléments de l'identité stable, ces « coordonnées sociales » déjà bien connues du système juridiques, faiblement variables au cours de l'existence, qui pointent vers une et une seule personne physique (I). Autour de ce noyau s'agglomère la pulpe du fruit : un univers infini d'informations extrêmement variables dans leur importance, leur nature, leur support, leur caractère intime ou nuisible. On pourrait la qualifier « d'identité construite », mais le sens de cette expression doit être précisé. L'identité stable est un ensemble d'éléments donnés à l'individu à sa naissance. Leur modification par la suite est, au mieux extrêmement difficile, au pire impossible. L'identité construite, quant à elle, propose une vision — nécessairement partielle, déformée, exagérée, mouvante — du parcours de l'individu, de sa naissance à sa mort. C'est un récit, un journal. Mais il faut relever que, dans cet ensemble bigarré d'événements fondateurs et d'anecdotes, certains sont tout à fait extérieurs à la volonté de l'individu : le fait qu'il développe une maladie, perde un parent proche, soit victime d'un licenciement... Si cette identité est « construite », ce n'est pas tant par son acteur principal que par les forces de traitement numérique, qui en recueillent les traces et les assemblent (II). La manière dont la personne peut agir pour modeler la statue qu'on lui érige sera abordée à la section suivante.

I - Le centre : l'identité stable

34. **Se dissimuler, se révéler** - Nous verrons plus loin que l'identité stable joue un rôle à la fois hors-ligne et en ligne, comme substrat autour duquel viendra s'agglomérer l'ensemble des données à caractère personnel formant l'identité construite. Pour l'heure, nous évoquerons uniquement la présence en ligne. Lorsqu'un individu déploie des activités sur les réseaux, son identité stable est-elle connue de ceux qui mettent des contenus, des services à sa disposition ou qui échangent avec lui ? La réponse de principe est négative : l'identité est occultée (A). Ce n'est pas irrémédiable, et il est loisible aux internautes de révéler qui ils sont. Encore devront-ils convaincre leurs interlocuteurs (B).

A - L'identité occultée

35. **L'architecture du transfert de données** - Dans son ouvrage *Code and other laws of cyberspace*, M. Lessig insiste sur les conséquences juridiques des choix techniques et architecturaux réalisés par les ingénieurs à l'origine d'Internet⁴². L'anonymat par défaut des internautes est en est une parfaite illustration.

[...] the Internet is built from a suite of protocols referred to collectively as "TCP/IP." At its core, the TCP/IP suite includes protocols for exchanging packets of data between two machines "on" the Net. Brutally simplified, the system takes a bunch of data (a file, for example), chops it up into packets, and slaps on the address to which the packet is to be sent and the address from which it is sent. The addresses are called Internet Protocol addresses, and they look like this: 128.34.35.204. Once properly addressed, the packets are then sent across the Internet to their intended destination. Machines along the way ("routers") look at the address to which the packet is sent, and depending upon an (increasingly complicated) algorithm, the machines decide to which machine the packet should be sent next⁴³.

Pour être transmis sur les réseaux, le paquet contenant une information à transmettre a donc besoin d'être « étiqueté » par deux données externes : l'adresse IP expéditrice, et l'adresse IP destinataire. Les adresses IP correspondent à des machines ou à des ensembles de machines connectées au réseau⁴⁴. Elles sont attribuées par les fournisseurs d'accès à Internet (FAI). Le destinataire du paquet d'information n'a pas la possibilité de savoir à quel abonné est attribuée une adresse IP donnée à un moment donné : seul le FAI est capable de le dire. Il peut certes être contraint de révéler à la justice qui est cet abonné, et nous aurons l'occasion d'y revenir. Mais l'hypothèse reste exceptionnelle. L'anonymat est bien la règle, et cette règle correspond à un choix architectural délibéré :

This minimalism in the Internet's design was not an accident. It reflects a decision about how best to design a network to perform a wide range over very different functions. Rather than build into this network a complex set of functionality thought to be needed by every single application, this network philosophy pushes complexity to the edge of the network—to the applications that run on the network, rather than the network's core. The core is kept as simple as possible. Thus if authentication about who is using the network is necessary, that functionality should be performed by an application connected to the network, not by the network itself⁴⁵.

42. - V.supra, n°21.

43. - L. Lessig, *Code V2*, op. cit., p. 43.

44. - Une seule adresse IP publique peut en effet renvoyer, en réalité, à plusieurs machines constituant un réseau domestique ou d'entreprise. Un routeur est alors chargé de distribuer correctement les paquets à l'intérieur du réseau local.

45. - *Ibid.*, p. 44.

36. L'avantage technique : le caractère évolutif d'Internet - Permettre à n'importe quelle machine et à n'importe quel utilisateur humain de se présenter sur le réseau et d'y communiquer sans se soucier de son identité, c'est faire le choix d'une plasticité technique maximale, de nature à favoriser l'innovation. Les inventeurs des protocoles collectivement connus sous le nom de TCP/IP ont urni une boîte à outils, que d'autres ont employée par la suite en y superposant de nouvelles couches de protocoles. Les plus connus sont FTP pour le transfert de fichiers, SMTP pour l'envoi d'emails, HTTP pour la publication de documents contenant des liens hypertextes, autrement dit de pages Web⁴⁶. Encore un niveau plus haut, ces protocoles sont exploités par des navigateurs Internet, des objets connectés, des applications pour téléphones intelligents, et ainsi de suite. Il revient à ces couches supérieures du réseau de se soucier de *qui* envoie des paquets d'information sur Internet, et du *contenu* de ces paquets, dans la stricte mesure de ce que les concepteurs de ces couches supérieures auront décidé. Faire peser ces contraintes sur les couches profondes du réseau aurait réduit drastiquement la capacité des inventeurs du monde entier à en proposer de nouveaux usages⁴⁷.

37. L'avantage social : la liberté d'expression et de navigation - Héritiers de ces choix techniques fondateurs, la plupart des usages courant d'Internet restent aujourd'hui anonymes. Mais comme le souligne M. Lessig, rien n'empêche techniquement d'aller contre cette tendance dans la conception des couches supérieures du réseau, voire même de modifier l'architecture profonde d'Internet. Est-ce souhaitable ? Les dangers de l'anonymat, aux yeux d'un juriste, sont évidents. Il facilite la commission d'infractions en toute impunité, et l'on pense aussitôt aux violations massives du droit d'auteur, ou aux multiples abus de la liberté d'expression que l'on constate chaque jour en ligne. Soulignons d'emblée, toutefois, que les autorités disposent de plusieurs moyens efficaces de briser l'anonymat, dont celui, déjà évoqué, qui consiste à forcer le fournisseur d'accès à Internet à rapprocher l'adresse IP d'un délinquant de son répertoire d'abonnés.

Ces levées ponctuelles d'anonymat sont largement préférables à une identification systématique et généralisée. Un arrêt rendu en 2011 par la cour d'appel de Hamm, en Allemagne, explique fort bien pourquoi. Cette juridiction avait été saisie par un psychothérapeute, mécontent de la note médiocre qui lui avait été attribuée par un ancien patient sur une plateforme de notation en ligne⁴⁸. Son recours a été rejeté, la juridiction estimant que l'obligation d'assortir une opinion particulière

46. - *Ibid.*, p. 144.

47. - *Ibid.*, p. 112.

48. - Arrêt I-3 U 196/10 du 3 août 2011, consultable sur <http://www.justiz.nrw.de>. V. le commentaire de cette décision dans A. Schmitt, « Existe-t-il un droit à l'anonymat sur Internet ? », article *unpeudedroit.fr* du 13 décembre 2014.

de son nom risquerait de conduire les individus à ne pas exprimer leurs opinions, par crainte de représailles. Elle ajoute que ce risque d'autocensure irait à l'encontre du droit fondamental à la libre expression⁴⁹.

La Cour européenne des Droits de l'Homme a formulé des remarques similaires au détour d'un arrêt rendu par sa Grande chambre en 2015⁵⁰. Des menaces et remarques diffamatoires avaient été placées en commentaires sous un article de presse, sur le site d'un journal estonien. Les propos tenus étaient nettement illicites, et la responsabilité de leurs auteurs méritait d'être engagée. L'essentiel de la discussion portait d'ailleurs sur la responsabilité de la société éditrice du site Internet. Constituent donc un *obiter dictum* les affirmations : « L'anonymat est de longue date un moyen d'éviter les représailles ou l'attention non voulue. En tant que tel, il est de nature à favoriser grandement la libre circulation des informations et des idées, notamment sur Internet ».

Des études empiriques vont dans le même sens. Elles démontrent que les internautes ont modifié leur comportement à la suite des révélations d'Edward Snowden relatives aux pratiques de surveillance massive par des agences de renseignement américaines. Deux articles, en particulier, décrivent ce « *chilling effect* » et s'attachent à le mesurer d'un point de vue statistique. L'une porte sur la tendance des internautes à s'autocensurer lorsqu'ils craignent d'être surveillés et estiment que les opinions politiques qu'ils souhaiteraient exprimer sont minoritaires⁵¹. L'autre porte sur la simple consultation passive d'informations : elle démontre que la fréquentation des pages Wikipédia considérées comme « sensibles » (celles, notamment, liées à des thématiques terroristes) a diminué de manière significative depuis la révélation du programme *Prism*⁵².

38. Identités virtuelles - Internet procure un anonymat par défaut de ses utilisateurs. En cela, s'oppose-t-il en totalité à l'existence « hors-ligne » ? Sans doute pas : échanger quelques mots avec ses semblables dans la rue, dans un bar, passer de petits contrats (acheter un journal par exemple) ne requiert pas de révéler son identité stable. De telles interactions sociales révèlent certes des éléments partiellement identifiants, comme l'apparence physique, mais l'internaute révèle aussi un fragment d'identification à travers son adresse IP. Nous verrons par la suite comment ces traces peuvent être exploitées pour découvrir quelle identité stable elles dissimulent. Pour l'instant,

49. - « *Die Verpflichtung, sich namentlich zu einer bestimmten Meinung zu bekennen, würde allgemein die Gefahr begründen, dass der Einzelne aus Furcht vor Repressalien oder sonstigen negativen Auswirkungen sich dahingehend entscheidet, seine Meinung nicht zu äußern. Dieser Gefahr der Selbstzensur soll durch das Grundrecht auf freie Meinungsäußerung entgegen gewirkt werden* ».

50. - CEDH, 16 juin 2015, *Delfi AS c. Estonie*, 64569/09.

51. - E. Stoycheff, « Under surveillance: examining Facebook's spiral of silence effects in the wake of NSA Internet monitoring », *Journalism & Mass Communication Quarterly*, 2016, vol. 93(2), p. 296.

52. - J. W. Penney, « Chilling effects : online surveillance and Wikipédia use », *Berkeley Technology Law Journal*, 2016, vol : 31:1, p. 117.

laissons de côté cette possibilité et postulons que la navigation et l'expression sont anonymes. La comparaison avec le monde « hors-ligne » a ses limites, et il faut reconnaître que l'anonymat est plus massivement et plus durablement présent en ligne. L'explication n'est pas seulement technique : elle est aussi culturelle. Si un individu fréquente assidument un club de discussion ou de lecture « hors-ligne », il lui sera rapidement demandé de se présenter. À ce moment, l'utilisation d'un pseudonyme fantaisiste serait certainement mal perçue ; l'utilisation d'un nom d'emprunt crédible quoique mensonger serait envisageable, mais ne viendrait que rarement à l'esprit des individus et, si elle est découverte, elle sera vécue comme une trahison par leurs interlocuteurs, provoquant des réactions d'incompréhension, voire d'hostilité. En ligne, l'anonymat et le pseudonymat sont facilement tolérés, voire recherchés. Dans certains espaces virtuels, cohabitent des intervenants sous leur nom propre et d'autres sous pseudonymes : c'est le cas des commentaires sous les articles de presse, ou de certains forums de discussion. D'autres forums en revanche, de même que la plupart des jeux vidéo en ligne, reposent sur une culture généralisée de l'anonymat. À l'exact inverse de notre club de lecture « hors-ligne », celui qui y interviendrait sous son véritable nom provoquerait la surprise, et sans doute l'incompréhension.

La combinaison des facilités techniques et culturelles offertes par Internet pour recourir à l'anonymat et au pseudonymat produit de puissants effets psychologiques. C'est l'occasion, pour l'individu, de « faire comme si », pour quelques heures, il s'était débarrassé de son identité stable. M. Lessig décrit le choc culturel qu'a provoquée, chez les Américains, la proposition du fournisseur d'accès à Internet American Online (AOL) de naviguer, au sein de la communauté et des chats AOL, sous cinq identités différentes, qui pouvaient certes être attribuées chacune à un membre d'une famille, mais qui pouvaient également être toutes employées, alternativement, par le même individu.

So in AOL you were given a fantastic power of pseudonymity that the “code writers” of real space simply do not give. You could, of course, try in real space to live the same range of multiple lives, and to the extent that these lives are not incompatible or inconsistent, you could quite often get away with it. For instance, you could be a Cubs fan during the summer and an opera buff during the winter. But unless you take extraordinary steps to hide your identity, in real space you are always tied back to you. You cannot simply define a different character; you must make it, and more important (and difficult), you must sustain its separation from your original identity⁵³.

Une part de l'attrait d'Internet tient dans l'existence de ces espaces où l'on peut laisser son identité habituelle à l'entrée, comme un vêtement, pour la reprendre à la sortie. Néanmoins, ces individus devraient garder à l'esprit que leur « identité virtuelle » ne se détache pas totalement de

53. - L. Lessig., *Code V.2*, op. cit., p. 90.

leur identité civile. L'ensemble de ce qu'ils disent et font sous ces identités d'emprunts s'agglomère autour du noyau constitué par l'identité stable, sous forme de traces numériques, qui pourront être recensées et rattachées à eux par divers moyens qui seront examinés ultérieurement.

Il est temps d'examiner une hypothèse quelque peu différente : celle dans laquelle l'internaute, techniquement anonyme par défaut, *souhaite* faire usage de son identité stable. Il lui faudra alors convaincre ses interlocuteurs en ligne qu'il est bien celui qu'il prétend être. L'anonymat cesse d'être un atout et devient un obstacle, qu'il faut surmonter.

B - L'identité prouvée

39. Le besoin d'identité en ligne - Bien souvent, nous l'avons vu, l'internaute s'accommode de son anonymat. Mieux : il le recherche et le désire. Toutefois, le développement exponentiel du commerce électronique, des banques en ligne, des démarches administratives dématérialisées, des environnements numériques de travail, rendent nécessaire une « réidentification » ponctuelle de l'individu. Le droit d'accéder à certaines informations et à certains services, dans ces différentes hypothèses, n'est pas accordé à tout visiteur de manière indifférenciée. Il est réservé à certaines personnes, capables de faire la démonstration de leur identité stable. Elles seules ont le droit de consulter tel compte bancaire ou d'ordonner qu'il soit procédé à un virement ; de prendre connaissance d'un document couvert par le secret fiscal ; de lire des informations réservées aux employés d'une entreprise ou aux étudiants d'une université. La conclusion d'un contrat, quant à elle, n'appelle pas toujours une identification approfondie, ni hors-ligne — reprenons l'exemple de l'achat d'un journal au kiosque du coin — ni en ligne. Mais à côté des petits contrats de la vie quotidienne, il existe des conventions d'une importance substantielle, que l'on ne peut imaginer conclure sans avoir connaissance de la capacité de contracter, voire de l'identité civile complète de son partenaire.

Le besoin d'identification, d'ailleurs, est à double sens. La plateforme en ligne doit savoir, dans certaines hypothèses, qui est son utilisateur. Mais l'utilisateur doit s'assurer lui aussi qu'il traite bien avec la plateforme authentique, non avec un usurpateur. Les sites se faisant passer pour des marchands ou des établissements de crédit afin de dérober des données personnelles — au premier rang desquelles des données de paiement — sont malheureusement nombreux.

Or, nous l'avons vu, l'ensemble de protocoles appelé TCP/IP ne relie pas les expéditeurs ni les destinataires des paquets d'informations à des identités. Mais nous avons exposé également que ces tâches pouvaient être confiées à des protocoles supplémentaires, superposés au TCP/IP. Ces

protocoles existent et visent, dans le vocabulaire informatique, à l'authentification⁵⁴. Ils reposent tous, nécessairement, sur le chiffrement.

40. Le chiffrement, « Janus aux deux visages » - Le chiffrement a souvent mauvaise presse. Il sert fondamentalement à rendre une communication entre deux personnes incompréhensible pour tout observateur extérieur à leur relation. Il est dès lors perçu par une partie du personnel politique et du grand public comme un moyen de planifier des actions criminelles, en particulier terroristes, en échappant à la surveillance des services judiciaires et de renseignement. Après avoir qualifié le chiffrement de « Janus aux deux visages »⁵⁵, M. Lessig écrit ainsi :

[...] encryption can serve two fundamentally different ends. In its “confidentiality” function it can be “used to keep communications secret.” In its “identification” function it can be “used to provide forgery-proof digital identities.” It enables freedom from regulation (as it enhances confidentiality), but it can also enable more efficient regulation (as it enhances identification)⁵⁶.

Dans sa fonction d'authentification, le chiffrement n'est donc pas l'adversaire du droit, mais plutôt son auxiliaire. Il permet de procéder aux « contrôles d'identité » en ligne. Il substitue à d'imparfaites « traces numériques », comme l'adresse IP, des mécanismes de nature à susciter une confiance bien plus élevée qu'on traite avec un tel individu, relié à telle identité stable. Il nous paraît fondamental de nous attarder suffisamment sur ces services indispensables rendus au droit par le chiffrement. Ces éléments seront cruciaux lorsque nous aborderons, plus loin, l'attitude générale (hostilité ou protection) que doit adopter le système juridique à l'endroit de ces techniques.

Pour comprendre comment il est possible à deux entités (personnes, entreprises) de communiquer sur Internet en s'assurant de leurs identités réciproques, il faut rappeler au préalable les grandes lignes de fonctionnement du chiffrement.

Le chiffrement « symétrique », déjà employé en Égypte ou dans la Rome antique, permet de rendre une communication entre A et B indéchiffrable par C en utilisant une « clé » unique, qui sert tout à la fois à chiffrer et à déchiffrer les contenus. Le système présente un inconvénient majeur :

54. - « L'authentification a pour but de vérifier l'identité dont une entité (personne ou machine) se réclame. Généralement, l'authentification est précédée d'une identification qui permet à cette entité de se faire reconnaître du système par un élément dont on l'a doté. En résumé, s'identifier c'est communiquer une identité préalablement enregistrée, s'authentifier c'est apporter la preuve de cette identité » (« Authentification. Règles et recommandations concernant les mécanismes d'authentification de niveau de robustesse standard », circulaire Direction centrale de la sécurité des systèmes d'information N° 729/SGDN/DCSSI/SDS/AsTeC). Le mot « identification », en droit, recouvre donc à la fois l'identification au sens informatique (la déclaration qu'on entend se prévaloir d'une identité donnée) et l'authentification (la preuve que l'on est bien celui qu'on prétend être).

55. - « *It thus demonstrates the sense in which cryptography is Janus-faced* » (L. Lessig., *Code V.2, op. cit.*, p. 53).

56. - *Ibid.*

ladite clé ne peut pas voyager avec le message chiffré, car un tiers qui intercepterait ces deux éléments serait aussitôt en mesure de percer le secret. Ce système n'est donc acceptable que si la clé peut être communiquée par un canal sécurisé, par exemple par remise en mains propres entre A et B avant qu'ils s'éloignent et entament la communication. À l'heure d'Internet, une remise de clé symétrique pourrait par exemple s'effectuer par courrier postal avant que la communication ne s'établisse ensuite sur le réseau.

La découverte du système de chiffrement « asymétrique », par messieurs Diffie et Hellmann, au milieu des années 70, a constitué un progrès considérable. Il repose sur l'existence de fonctions mathématiques dites « à sens unique », qui sont très faciles à appliquer dans un sens, mais qu'il est extrêmement difficile d'exécuter en sens inverse... à moins de disposer d'une information supplémentaire, qualifiée en mathématiques de « brèche secrète ». Chaque utilisateur d'un chiffrement asymétrique va donc créer une paire de clés de chiffrement. La première clé est dite « clé publique », et peut être révélée par A au monde entier. Elle permettra à toute personne B qui souhaite envoyer un message secret à A d'y appliquer la fonction mathématique « à sens unique ». La seconde clé est dite « clé privée ». A ne va la révéler à personne. Elle constitue la fameuse « brèche secrète » qui lui permettra, et à lui seul, d'appliquer la fonction mathématique en sens inverse, c'est-à-dire de déchiffrer le message. Le génie de ce système, c'est qu'il permet à des personnes ne s'étant jamais rencontrées et n'ayant jamais communiqué « hors Internet » d'entamer immédiatement une communication chiffrée, en échangeant leurs clés publiques, tout en celant leurs clés privées. Un attaquant qui intercepterait les clés publiques ne pourrait rien en faire.

Ces grands principes ayant été rappelés, nous pouvons décrire schématiquement la manière dont un individu peut faire la preuve de son identité stable. Encore faut-il au préalable que l'individu, qui sera le plus souvent à l'origine de la connexion, soit lui-même certain qu'il traite avec la bonne entité.

41. L'authentification de la plateforme - Le *Transport Layer Security* (TLS) est un protocole fréquemment employé lorsqu'il s'agit d'établir une connexion entre un client (la personne qui cherche à accéder à un service en ligne) et un serveur. Il sert à la fois à authentifier le serveur et à chiffrer le contenu des échanges. Il faut bien comprendre que ces deux fonctions sont indissociables : si la communication s'effectuait « en clair », il n'y aurait par exemple aucun moyen de s'assurer qu'un attaquant ne s'est pas interposé entre, disons, la banque et son client. Il suffirait à ce tiers hostile de se placer au milieu de l'échange, de l'écouter tout en le relayant, et il mettrait la main sur l'ensemble des données sensibles. Ce procédé est désigné, en sécurité informatique, sous le nom « d'attaque de l'homme du milieu ».

Pour qu'une plateforme communique avec ses utilisateurs de manière sécurisée, il faut donc qu'elle diffuse sa « clé publique ». Cette clé pourra être employée par le correspondant pour adresser à la banque, à l'administration, au commerçant, des données dont lui seul pourra prendre connaissance. Mais comment éviter qu'une fausse plateforme ne tende un piège à l'ensemble des internautes, en diffusant une autre clé publique ? Un nouvel acteur doit être intégré dans l'opération : un tiers de confiance appelé « autorité de certification ». Ces autorités sont des structures privées, qui ont pour mission d'échanger « hors-ligne » avec les plateformes qui souhaitent utiliser le protocole TLS. L'autorité s'assure (par des échanges téléphoniques, de courriers traditionnels...) de l'identité de la plateforme, et vérifie qu'elle est bien en train de correspondre avec d'authentiques représentants. Si tel est le cas, elle intègre la clé publique qui lui est présentée par la plateforme dans un document électronique, auquel elle applique son propre chiffrement. Le résultat de cette opération est un document numérique appelé « certificat », qui est placé sur le site Internet de la plateforme.

Lorsque le navigateur d'un internaute accède à un site tel que <https://www.impots.gouv.fr>, il prend connaissance du certificat. Il se tourne vers une autorité de certification et lui demande si ce certificat émane bien d'elle. L'autorité déchiffre le certificat, constate qu'il est authentique, et donne instruction au navigateur d'utiliser la clé publique de la plateforme pour établir une connexion sécurisée. C'est ainsi que l'on procède à la vérification des identités en ligne, s'agissant des administrations et grands acteurs privés susceptibles de recevoir la visite d'un large public.

42. L'authentification du visiteur - Une fois le dialogue sécurisé établi se pose la question qui nous intéresse à titre principal : comment vérifier l'identité du visiteur ? En France, il n'existe pas de système global d'identification « hors-ligne » suivi de la fourniture d'un certificat numérique individuel. Autrement dit, la procédure décrite pour vérifier l'identité des plateformes n'est pas transposée aux individus. La valeur identifiante d'un simple formulaire déclaratif, comme on trouve partout sur Internet, est presque nulle. Une telle déclaration unilatérale ne saurait suffire lorsque l'identification est un préalable à l'échange d'informations sensibles, ou à la conclusion d'opérations ayant des conséquences juridiques sérieuses.

Comme le rappelle l'Agence nationale de la sécurité des systèmes d'information (ANSSI), il est possible de s'assurer de l'identité d'un interlocuteur à l'aide de trois séries d'informations. On s'appuiera sur « quelque chose qu'il sait » (un identifiant, un mot de passe, une signature...), « quelque chose qu'il possède » (une carte à puce, une carte magnétique, un téléphone sur lequel est reçu un SMS...), ou « quelque chose qu'il est » (une caractéristique biométrique, comme une

empreinte digitale ou une reconnaissance rétinienne)⁵⁷. Il faut souligner qu’aucun de ces procédés n’offre une sécurité parfaite. Le choix du facteur d’identification, et surtout le recours à un facteur isolé ou à une combinaison de plusieurs facteurs, modifie cependant la fiabilité du résultat de manière très significative. Ainsi, hors-ligne, exiger uniquement une signature autographe offre une sécurité très faible, car le savoir-faire nécessaire à l’imitation n’est pas d’un accès très difficile. Si l’on exige de surcroît la présentation d’une pièce d’identité, on ajoute deux tests supplémentaires : l’un basé sur « ce que l’individu possède » (a-t-il le document ?) et l’autre sur « ce qu’il est » (ressemble-t-il à la photographie ?).

En ligne, quel est le niveau d’exigence couramment constaté ? Le dispositif « France Connect » constitue un exemple intéressant. Il s’agit d’un système développé par les pouvoirs publics français et qui permet, après une identification en un point unique, d’accéder à un univers de services administratifs en ligne : consultation du solde de points du permis de conduire, simulation de retraite, accès au site à services multiples service-public.fr... Il suffit au citoyen d’exploiter un compte en ligne préexistant dont il disposerait auprès des impôts, de la sécurité sociale ou de La Poste⁵⁸. Ces trois derniers acteurs sont qualifiés de « fournisseurs d’identité » et transmettent au service auquel l’administré tente d’accéder un ensemble de six données « qui constituent son identité pivot, à savoir : son nom, son prénom, son sexe, sa date de naissance, son lieu de naissance, son pays de naissance »⁵⁹. Il s’agit bien de contrôler l’identité stable de l’internaute, de s’assurer de ses coordonnées sociales uniques. Or, comment crée-t-on un compte chez ces « fournisseurs d’identité » ? En utilisant des données préalablement reçues par courrier papier⁶⁰. Sur impots.gouv.fr, il faut combiner des données issues de la dernière déclaration de revenus (numéro fiscal et numéro de déclarant en ligne) et avis d’impôt sur le revenu (revenu fiscal de référence)⁶¹. Toutefois, la prise de contrôle par un pirate de l’adresse email du contribuable suffira à accéder aux données fiscales (et à l’ensemble de l’espace France Connect), en utilisant successivement les champs « numéro fiscal oublié » puis « mot de passe oublié ». Il ne s’agit pas, toutefois, d’une maladresse de la part de l’administration, mais bien d’un arbitrage conscient et délicat entre robustesse du système et facilité d’emploi pour les usagers. Encourager le développement des formalités administratives en ligne supposait sans doute de ne pas imposer aux citoyens des procédures d’authentification trop lourdes et trop pénibles.

57. - ANSSI, *Guide d’hygiène informatique*, version 2.0, janvier 2017, p. 19 : https://www.ssi.gouv.fr/uploads/2017/01/guide_hygiene_informatique_anssi.pdf

58. - Voir sur franceconnect.gouv.fr.

59. - <https://www.service-public.fr/particuliers/actualites/A10798>.

60. - Reçu sous forme de lettre simple, sans signature.

61. - V. la page d’accueil sur <https://cfspart.impots.gouv.fr/>.

Les acteurs privés exigeants en matière de sécurité comme les banques commencent par fournir des identifiants en mains propres ou par courrier postal. Puis, pour la passation d'opérations sensibles comme des virements à des nouveaux bénéficiaires, elles ajoutent un facteur supplémentaire d'identification, généralement la fourniture d'un code reçu par SMS ou affiché dans une application pour téléphone intelligent⁶².

S'agissant du commerce en ligne, la vérification de l'identité stable de l'individu est bien plus laxiste. Comme nous le verrons lorsque nous envisagerons le droit des contrats à l'ère numérique, le commerçant se contente généralement d'une déclaration unilatérale d'identité, qui peut être purement fantaisiste. S'il s'agit de livrer un bien physique, il peut compter, dans une certaine mesure, sur la nécessité de fournir une adresse postale réelle. Surtout, dans tous les cas où l'internaute doit payer, le mode de paiement est susceptible de créer un lien avec son identité stable. Nous verrons cependant que ce lien est ténu : le paiement du prix peut avoir été offert à l'internaute par un tiers, qui fournira ses données de paiement mais ne sera pas le contractant à strictement parler ; surtout, les données de paiement peuvent avoir été dérobées. L'identité est donc mal révélée par le fonctionnement du commerce électronique.

Rappelons enfin que la plupart des services gratuits sur Internet ne procèdent à aucun lien sérieux entre l'identité prétendue et la véritable identité stable de l'internaute. Ainsi, sur le réseau social Twitter, chacun peut afficher les nom et qualité de son choix. Seuls les comptes rattachés à des institutions ou à des célébrités font l'objet d'une vérification, par l'intermédiaire de procédés « hors-ligne » : ils sont signalés par une petite coche blanche sur fond bleu. Les autres permettent librement l'utilisation de pseudonymes, mais présentent aussi le risque d'usurpation de l'identité d'un autre individu.

43. La protection pénale de l'identité numérique - Le fait que l'on puisse brandir, sur les réseaux, une identité existante, mais qui n'est pas la sienne, est de nature à gravement perturber l'ordre social. C'est pourquoi un tel comportement a été incriminé à l'article 226-4-1 du Code pénal :

Le fait d'usurper l'identité d'un tiers ou de faire usage d'une ou plusieurs données de toute nature permettant de l'identifier en vue de troubler sa tranquillité ou celle d'autrui, ou de porter atteinte à son honneur ou à sa considération, est puni d'un an d'emprisonnement et de 15 000 € d'amende.

Cette infraction est punie des mêmes peines lorsqu'elle est commise sur un réseau de communication au public en ligne.

62. - V. par ex. le système de « clé digitale » de BNP Paribas : <https://mabanque.bnpparibas/fr/notre-offre/comptes-cartes-et-services/gerer-ses-comptes-et-son-budget/gerer-ses-comptes-en-ligne/cle-digitale>.

Ce texte est issu d'une loi du 14 mars 2011⁶³. Auparavant, les usurpations d'identité n'étaient sanctionnées que lorsqu'elles entraient dans le champ d'application de l'article 434-23 qui dispose :

Le fait de prendre le nom d'un tiers, dans des circonstances qui ont déterminé ou auraient pu déterminer contre celui-ci des poursuites pénales, est puni de cinq ans d'emprisonnement et de 75 000 euros d'amende.

Nonobstant les dispositions des articles 132-2 à 132-5, les peines prononcées pour ce délit se cumulent, sans possibilité de confusion, avec celles qui auront été prononcées pour l'infraction à l'occasion de laquelle l'usurpation a été commise.

Est punie des peines prévues par le premier alinéa la fausse déclaration relative à l'état civil d'une personne, qui a déterminé ou aurait pu déterminer des poursuites pénales contre un tiers.

Par conséquent, avant la loi de 2011, « [...] l'usurpation du nom d'une personne n'ayant pas pour effet d'entraîner d'éventuelles poursuites pénales à son encontre échappait à toute condamnation, tout comme le fait d'emprunter non pas le nom d'un tiers, mais d'autres éléments se rapportant à lui tels qu'une adresse électronique, un nom de domaine, un pseudonyme utilisé sur une plateforme d'échanges, etc ⁶⁴. Lorsque ces éléments d'apparence secondaire pointent vers une identité stable (« ...données de nature à l'identifier... »), il est justifié de leur accorder une protection.

L'article 226-4-1 du Code pénal a déjà été appliqué, par exemple, à une personne ayant créé de faux profils Facebook au nom d'autrui, au contenu diffamatoire⁶⁵, ou à celle ayant pris le contrôle du site Internet d'une personnalité politique pour y afficher de faux communiqués présentés comme authentiques⁶⁶. On remarquera que l'usurpation d'identité s'accompagne souvent d'une autre infraction : dans le premier exemple, la diffamation ; dans le second, l'introduction dans un système automatisé de traitement de données⁶⁷. Quant à l'usurpation d'identité numérique qui viserait par exemple à prendre le contrôle d'une interface bancaire pour y procéder à un virement à son bénéfice, il s'agirait d'une escroquerie, celle-ci étant définie par l'article 313-1 du Code pénal comme :

« le fait, soit par l'usage d'un faux nom ou d'une fausse qualité, [...] de tromper une personne physique ou morale et de la déterminer ainsi, à son préjudice ou au préjudice d'un tiers, à remettre des fonds, des valeurs ou un bien quelconque, à fournir un service ou à consentir un acte opérant obligation ou décharge ».

63. - Art. 2 de la loi n° 2011-267 du 14 mars 2011 d'orientation et de programmation pour la performance de la sécurité intérieure. Sur texte, V. not. F. Mattatia, « L'usurpation d'identité sur Internet dans tous ses états », *RSC*, 2014, p. 331.

64. - E. A. Caprioli, obs. sur CA Paris, 10 oct. 2014, n° 13/7387, *CCE*, déc. 2015, comm. 9.

65. - CA Paris, 10 oct. 2014 : obs. préc. E. Caprioli.

66. - TGI Paris, 18 déc. 2014, n° 12010064012 : *Lexisnexus* 360, 27/01/15, obs. O. Flipo.

67. - Art. 323-3. C. pén.

Enfin, dans les rapports avec l'administration en ligne, l'article 433-19 du Code pénal pourrait trouver à s'appliquer :

Est puni de six mois d'emprisonnement et de 7 500 euros d'amende le fait, dans un acte public ou authentique ou dans un document administratif destiné à l'autorité publique et hors les cas où la réglementation en vigueur autorise à souscrire ces actes ou documents sous un état civil d'emprunt :

1° De prendre un nom ou un accessoire du nom autre que celui assigné par l'état civil ;

2° De changer, altérer ou modifier le nom ou l'accessoire du nom assigné par l'état civil.

44. La carte d'identité électronique : prouver mieux ? - En dépit de cet arsenal pénal, qui semble assez complet, un rapport gouvernemental sur la cybercriminalité présente le chiffre très impressionnant de 300 000 usurpations d'identité par an, dont la plupart en ligne. À cela s'ajoutent des dégâts invisibles et difficilement quantifiables : les usages numériques dont la croissance sera ralentie, voire empêchée, faute de mécanismes d'identification suffisamment fiables en ligne.

Dans un tel contexte, certains pays adoptent des solutions censées procurer à la fois un haut niveau de fiabilité, et un très large éventail d'utilisations en ligne. C'est notamment le cas des cartes d'identité électroniques, mises en place dans des pays tels que la Belgique, l'Espagne, le Portugal, l'Italie, la Suède, la Finlande, l'Estonie, la Lituanie ou encore Monaco⁶⁸. Il s'agit d'un titre d'identité qui sert à la fois « hors-ligne » et « en ligne ». Les citoyens belges, par exemple, insèrent cette carte dans un lecteur connecté à leur ordinateur afin d'accéder à leur espace fiscal en ligne ou à leur dossier médical⁶⁹. La puce contient des « certificats » du même type que ceux qui sont octroyés aux plateformes dans le cadre de l'utilisation du protocole TLS⁷⁰. L'État joue le rôle d'autorité de certification et fournit aux tiers qui traiteraient, en ligne, avec un citoyen belge, une preuve solide de leur identité, grâce au chiffrement. Ces certificats peuvent également servir à apposer une signature électronique sur un document.

Naturellement, il ne suffit pas d'insérer la carte dans le lecteur pour s'en servir. Un deuxième facteur d'authentification est requis, afin qu'une carte dérobée ne puisse être employée. Le choix des autorités belges s'est porté sur un code PIN, d'une longueur maximale de 16 chiffres, avec blocage de la carte si trois codes incorrects sont saisis à la suite. Un système d'opposition en cas de perte ou de vol complète le dispositif, sur un modèle général dont on aura compris qu'il est calqué

68. - E. Caprioli, F. Mattatia et S. Vulliet-Tavernier, « L'identité numérique. Entretien », *Cahiers de droit de l'entreprise*, mai 2011, entretien 3.

69. - Toutes les caractéristiques décrites ci-après sont énumérées sur le site officiel www.eid.be.

70. - V. supra n°41.

sur les cartes bancaires. Le choix d'un code PIN semble judicieux, à l'heure où l'authentification biométrique, et notamment par empreinte digitale, se développe à vive allure, notamment pour déverrouiller les téléphones intelligents. La CNIL rappelle « qu'il est possible de se procurer, sur de nombreux sites Internet et à faible coût, des « kits » permettant de relever des empreintes digitales ; que plusieurs études ont permis de démontrer la possibilité de frauder en trompant le lecteur d'empreintes grâce à un « faux doigt »⁷¹. Une personne dont les empreintes auraient été dérobées, dans un monde où ces traces serviraient de sésame généralisé en ligne et hors-ligne, se trouverait dans une situation inextricable. Un code PIN ou un mot de passe perdu ou volé peut toujours être renouvelé ; l'extrémité de l'index est irremplaçable. De même, il faut approuver le choix des autorités belges d'avoir stocké les informations sensibles sur chaque carte considérée individuellement, plutôt que de constituer une base de données centralisée qui serait interrogée à distance à chaque fois qu'un citoyen demande à être identifié. En effet, une telle base de données constituerait une cible de choix pour des pirates.

La France ne dispose pour l'heure d'aucune forme de carte d'identité destinée à une utilisation en ligne. En revanche, elle a précisément décidé de constituer un gigantesque fichier rempli d'informations biométriques. Au prétexte de sécuriser les demandes de délivrance et de renouvellement des titres d'identité traditionnels, un décret du 28 octobre 2016, dit « TES » pour « titres électroniques sécurisés », a décidé de la fusion des bases de données relatives aux cartes d'identité et aux passeports⁷². Le Conseil national du numérique (CNNum) a rendu un avis dans lequel il souligne à la fois l'intérêt que suscitera un tel fichier pour les agresseurs extérieurs, et les risques qu'un gouvernement ne décide de détourner les finalités de ce gisement de données, pour le livrer à la police ou aux services de renseignement. Le CNNum écrit par exemple : « Au regard de l'avis exprimé par la CNIL, le Conseil s'interroge sur la possibilité laissée par le décret d'utiliser un dispositif de reconnaissance faciale à partir de l'image numérisée de la photographie. Sur ce point, il importe de noter que les services de polices nationale et judiciaire, de gendarmerie et de renseignement peuvent d'ores et déjà accéder — aux termes de l'article 4 du décret — à l'image numérisée de la photographie enregistrée dans la base “pour les besoins exclusifs de leurs missions de prévention et de répression des atteintes aux intérêts fondamentaux de la Nation et des actes de terrorisme” »⁷³. Le CNNum demande donc, à juste titre, que les données de chaque individu soient

71. - CNIL, *Communication relative à la mise en œuvre de dispositifs de reconnaissance par empreinte digitale avec stockage dans une base de données*, p. 4 : <https://www.cnil.fr/sites/default/files/typo/document/Communication-biometrie.pdf>.

72. - Décret n° 2016-1460 du 28 octobre 2016 autorisant la création d'un traitement de données à caractère personnel relatif aux passeports et aux cartes nationales d'identité.

73. - Conseil national du numérique, *Avis sur le fichier TES*, décembre 2016, p. 11. Le document est consultable sur cnnumerique.fr.

stockées sur sa carte et là seulement : ce choix architectural permet des contrôles d'identité efficaces, tout en répondant aux autres objections.

45. La carte d'identité électronique : prouver moins ? - Les autorités belges ont évité ce piège de la base de données centralisée en concevant leur titre d'identité électronique. Cela ne suffit pas à apaiser toutes les craintes. La branche belge de la Ligue des droits de l'Homme a rendu un rapport appelant à la plus grande vigilance dans le développement de ces technologies⁷⁴. L'un de ses principaux reproches est le suivant : alors que présenter une carte d'identité classique était un geste sortant de l'ordinaire, il risque de devenir banal et quotidien si l'accès à de nombreux services en ligne y est conditionné. On allumerait son ordinateur et, dans la foulée, on y insérerait sa carte électronique, divulguant sans cesse l'essentiel de son identité stable à des interlocuteurs publics, mais aussi privés. Cette crainte n'est pas sans fondement. Ce n'est pas parce qu'il devient *possible* de délivrer une preuve solide de son identité stable que cela est toujours *souhaitable*. Si l'anonymat permanent n'est pas une solution viable, l'identification permanente ne l'est pas davantage. Personne n'accepterait de se promener en permanence avec sa carte d'identité épinglée à la poitrine.

Entre ces deux situations extrêmes, M. Lessig estime que les autorités publiques devraient promouvoir des solutions de « moindre identification ». L'auteur décrit le problème de l'identification excessive à partir de l'exemple d'un citoyen américain se présentant à un caissier avec de l'alcool. Il doit justifier être âgé de plus de 21 ans, et présente par conséquent un permis de conduire, qui fournit l'information demandée — le porteur a plus de 21 ans — mais bien davantage encore : l'âge exact, le nom, l'adresse et même, dans certains États fédérés, le numéro de sécurité sociale du client⁷⁵. S'agissant de l'identité en ligne, il imagine un système bien plus fin.

The virtual wallet would be different. If you need to authenticate your age, the technology could authenticate that fact alone—indeed, it could authenticate simply that you're over 21, or over 65, or under 18, without revealing anything more. Or if you need to authenticate your citizenship, that fact can be certified without revealing your name, or where you live, or your passport number. The technology is crafted to reveal just what you want it to reveal, without also revealing other stuff. (As one of the key architects for this metasystem, Kim Cameron, described it: "To me, that's the center of the system". And, most importantly, using the power of cryptography, the protocol makes it possible for the other side to be confident about the fact you reveal without requiring any more data.

Les utilisateurs de téléphones intelligents sont aujourd'hui accoutumés à un système « d'autorisations » de plus en plus fines. Il leur permet d'accorder ou de refuser l'accès d'une

74. - Ligue des droits de l'Homme, « Carte d'identité électronique : penser le progrès au lieu de le subir... » : http://www.liguedh.be/images/PDF/documentation/documents_thematiques/carte_identite_electronique.pdf.

75. - L. Lessig., *Code V.2*, op. cit., p. 51.

application donnée à leur carnet de contacts, à leur géolocalisation... L'idée d'accorder à des interlocuteurs en ligne un accès clair et plus ou moins profond à des couches de l'identité stable est séduisante. Certes, les défis techniques à relever ne manquent pas. Par exemple, les citoyens devraient être en mesure de vérifier que le logiciel qui accède aux informations d'identité et les transmet agit conformément à ce qu'il prétend. Cela implique notamment que son code source soit public, afin qu'il soit expertisé par les membres de la société civile disposant des compétences nécessaires. À supposer que ces difficultés soient surmontées, le résultat ouvrirait d'immenses possibilités en matière de réglementation. Prenons l'exemple des contenus pour adultes. Il est actuellement très facile au jeune public d'y accéder, ce qui entraîne de lourdes conséquences psychologiques, si l'on en croit les spécialistes⁷⁶. Si les internautes pouvaient ne pas révéler leur identité complète — ce à quoi l'on imagine bien qu'ils seraient réticents -, mais seulement le fait qu'ils ont ou pas dépassé l'âge de la majorité, il deviendrait socialement acceptable que l'État bloque les sites ne prévoyant pas cette révélation. En revanche, pour consulter son avis d'imposition, il faudrait toujours révéler son identité stable dans son entier.

Nous avons jusqu'ici considéré les rapports entretenus par le numérique avec les seuls éléments de l'identité stable. Il est temps d'élargir notre propos, en montrant comment les nouvelles technologies permettent d'agglomérer, autour de cette identité stable, une nuée de renseignements qui, pris isolément, sont moins identifiants. Rassemblés, ils forment cependant de l'individu un véritable « double numérique », parfois fidèle, parfois mensonger ; parfois précis, parfois illisible. Quoi qu'il en soit, nul ne peut plus ignorer l'existence de son avatar de chiffres et d'électrons.

II - La périphérie : l'identité construite

46. Le noyau et la chair - Les éléments constitutifs de l'identité stable sont les coordonnées sociales qui mènent à un unique citoyen et permettent de lui imputer les conséquences juridiques de ses actions. La liste de ces éléments n'est certes pas absolument immuable : le numéro NIR n'a pas toujours existé, et l'utilisation de certaines données biométriques comme moyens d'identification est récente. Mais ils restent peu nombreux et bien identifiés.

Au cours de son existence, il émane de la personne, à chaque instant, un ensemble hétéroclite d'informations anecdotiques ou fondamentales. Ce qu'elle fait ou s'abstient de faire, ce qui l'intéresse, qui elle rencontre, ce qu'elle dit et entend, où elle va, où elle porte son regard, les bonheurs qui la comblent et les malheurs qui la frappent, ce qu'elle croit et ce qu'elle veut : tout est

76. - Par ex. S. Kovacs, « Israël Nisand : la pornographie éduque les enfants à notre place », *lefigaro.fr*, 8 juillet 2015.

information. Jusqu'à une époque récente, la plupart de ces informations s'évaporaient dans l'air ambiant au fur et à mesure qu'elles apparaissaient, car elles n'étaient pas collectées, ni transcrites, ni conservées, ni rassemblées. Les systèmes numériques de traitement de l'information ont aujourd'hui des yeux et des oreilles partout. Ils n'oublient jamais, ou difficilement. Ils classent les informations, les trient, les recomposent pour les rendre facilement lisibles et exploitables.

L'information ne s'évapore plus. Aussitôt exsudée, elle est susceptible d'être remarquée, transcrite en une suite 1 et de 0, et placée dans une ou plusieurs bases de données. Ces fragments d'information s'enroulent autour de l'identité stable, sont pressés contre lui et y adhèrent pour ne plus le quitter. Autour du noyau se trouve à présent la chair, une nouvelle couche d'identité que l'on peut qualifier de « construite » - non par l'individu, mais par les systèmes de traitement de l'information. Nous verrons comment cette identité construite est née (A), puis comment elle s'est développée (B).

A - La naissance de l'identité construite

47. La prise de conscience - Au début des années 70, l'informatique personnelle n'existe pas encore, mais les outils de traitement de l'information se sont largement répandus dans des cadres professionnels, notamment dans les mains d'administrations publiques qui disposent depuis longtemps de considérables gisements de données sur leurs citoyens. Ces réservoirs d'information étaient cependant isolés les uns des autres. Or les voici tout à coup dotés d'une capacité à dialoguer : à croiser, à comparer et à rapprocher leurs contenus. Cette puissance nouvelle aux mains des pouvoirs publics, comme tout progrès technologique majeur, porte en son sein à la fois progrès et dangers. Les premières législations visant à encadrer les traitements d'information apparaissent en 1970 dans le Land de Hess, en 1973 en Suède, en 1974 aux États-Unis⁷⁷. En France, c'est l'affaire « SAFARI », bien connue, qui poussera les pouvoirs publics à agir. Les grands traits en sont rappelés ainsi par Guy Braibant :

En 1970, l'INSEE décide, semble-t-il de son propre chef, d'informatiser le répertoire d'identification et le numéro national d'identification de tous les Français. Ce répertoire, et le numéro qu'il contient avaient été créés par le « Service de la démographie » au printemps 1941, à partir des relevés des registres des actes de naissance généralement effectués par les greffiers des tribunaux de première instance [...]. Le but de cette informatisation était de parvenir à un identifiant unique pour les fichiers de toutes les administrations publiques et les caisses de la Sécurité sociale. Dans le même temps, le ministère de l'Intérieur s'apprêtait à mettre en œuvre un ordinateur très puissant destiné à la centralisation des bases de données que

77. - G. Braibant, *Données personnelles et société de l'information. Rapport au Premier ministre sur la transposition en droit français de la directive n° 95/46*, décembre 1998, p. 13.

*possédaient les services de police (dont les renseignements généraux, la direction de la sécurité du territoire, la police judiciaire). Or, le paradoxe que révélait l'article de Philippe Boucher ("Safari ou la chasse aux Français," paru dans Le Monde le 21 mars 1974) était que le Premier ministre avait écarté toute proposition de débat public sur les projets d'informatisation du gouvernement et ce, contrairement aux recommandations du Conseil d'État (rapport non publié de 1971) ou du ministère de la Justice, mais contrairement aussi aux gouvernements des pays voisins*⁷⁸.

L'article du Monde ayant fait scandale, une commission est constituée⁷⁹, qui rendra le 27 juin 1975 un rapport rédigé par le conseiller d'État Bernard Tricot et le professeur de droit Pierre Catala. Il faudra attendre le 6 janvier 1978 pour que naisse la loi dite « informatique et libertés »⁸⁰. Le rapporteur, l'ancien ministre de la Justice Jean Foyer, rappelle d'abord quels services immenses le traitement automatisé de l'information rend à la société : « Cette machinerie, elle-même inintelligente, a multiplié les moyens de l'intelligence humaine. Sans l'informatique, les hommes ne seraient pas allés dans la Lune »⁸¹. Mais il en décrit ensuite les dangers.

*Car l'ordinateur a une mémoire qui, à la différence de la mémoire des hommes, n'a pas la faculté d'oublier. Il n'oublie que ce qu'on efface en lui. Il est capable de sélectionner en quelques instants des données dont le recensement aurait demandé sans son aide peut-être des heures, des jours, voire des mois ou des années. Par des interconnexions entre ordinateurs, il devient possible de rassembler sur une question ou sur une personne une moisson énorme d'informations. [...] La conservation massive et systématique des données relatives à chaque personne tend aussi à juger les situations en attachant aux individus des étiquettes jadis plus rares et plus approximatives, et dont il leur était plus facile de se débarrasser. Est-il indispensable qu'on puisse savoir d'un homme de soixante ans qu'il était énurétique à trois ans, qu'il a contracté la coqueluche à huit ans, qu'il a échoué au baccalauréat à seize ans, qu'il a subi une punition durant son service militaire, qu'il a blessé un passant en voiture à vingt-cinq ans, qu'il a été licencié par un employeur à quarante ans et qu'il a subi une intervention chirurgicale à cinquante ans ?*⁸²

48. Le nouveau visage de l'information - Dès 1978, on dresse donc un constat dont la pertinence ne fera que croître jusqu'à nos jours : les mêmes informations ont une valeur, un potentiel, présentent des risques très différents selon la manière dont on les exploite. Lorsque les données étaient attachées à des feuilles de papiers, elles étaient périssables, et leur maniement d'une infinie lenteur. Regrouper un ensemble de savoirs administratifs ou privés attachés à un individu nécessitait une patience et des moyens rarement mis en œuvre pour un citoyen ordinaire.

78. - *Ibid.*, p. 14.

79. - Décret n°74-937 du 8 novembre 1974 instituant une commission chargée de proposer un code des libertés fondamentales de l'individu ; ayant pour objet de codifier les textes législatifs et réglementaires concernant l'exercice des libertés individuelles,

80. - Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

81. - Compte-rendu intégral de la séance de l'Assemblée nationale du 4 octobre 1977 : JO 1977-1978, p. 5782.

82. - *Ibid.*

L'écoulement du temps enterrait inexorablement les archives les plus anciennes sous des couches de poussière, les poussait vers le fond des placards, ou vers les broyeuses. L'époque de l'informatique est celle de l'hypermnésie, de la mise en ordre et de la consultation de données à la demande, en un claquement de doigts. « L'informatique, résumait encore Jean Foyer devant l'Assemblée nationale, présente des dangers pour la liberté, des dangers beaucoup plus grands que les anciens fichiers manuels ou mécanographiques. Il est des cas, en effet, dans lesquels la différence de degré se transforme en différence de nature »⁸³. S'il pressentait les progrès encore à venir, l'orateur ne pouvait imaginer leur ampleur ni la vitesse à laquelle ils seraient accomplis.

B - La montée en puissance de l'identité construite

49. **De l'information choisie à l'information totale** - Depuis les années 70, les modes de collecte des informations personnelles ont beaucoup évolué. La saisie manuelle était le mode principal d'alimentation des bases de données. Une fois numérisée, l'information devenait agile : elle pouvait être consultée, traitée ou transmise en quelques instants. Mais au moins le premier stade était-il affecté d'une certaine pesanteur, réduisant l'efficacité générale de la chaîne de traitement. Les bénéfices, mais aussi les risques de mauvais usages en étaient amoindris. Une information anodine ne pouvait pas faire l'objet d'une saisie manuelle. Les ressources humaines nécessaires à une telle saisie coûtent cher. Facteur aggravant : chaque fois qu'on élargit le spectre des informations recherchées, du plus fondamental vers le plus anecdotique, le nombre de données à aspirer augmente de manière exponentielle. Enfin, aux débuts de l'informatisation, on ne soupçonnait pas la valeur ajoutée qui peut être tirée d'un rapprochement à très grande échelle d'informations qui, prises isolément, n'ont aucun intérêt.

Désormais, c'en est fini des collectes laborieuses (1) et des traitements à courte vue (2).

1. - Une collecte généralisée

50. **La collecte en ligne : signaux, traces** - Aujourd'hui, une énorme masse de données est accumulée par des machines, à chaque seconde qui passe, en toute autonomie. L'on songe immédiatement aux données circulant en ligne : requêtes adressées aux moteurs de recherche, publications sur les blogs et réseaux sociaux, échanges de courriers électroniques... M. Dominique Cardon relève ainsi que « si l'on numérisait toutes les communications et les écrits depuis l'aube de

83. - *Ibid.*

l'humanité jusqu'en 2003, il faudrait 5 milliards de gigabits pour les mettre en mémoire. Aujourd'hui, nous générons ce volume d'informations numériques en deux jours ! »⁸⁴.

Lorsque l'information est fournie par l'internaute directement au prestataire qui entend l'exploiter, celui-ci n'a qu'à attendre et laisser les contenus s'accumuler dans ses bases de données. C'est le cas des réseaux sociaux, comme Facebook. Mais les géants d'Internet ne s'en tiennent pas là et lancent leurs robots d'exploration (les *crawlers*) sur l'ensemble des pages publiquement accessibles à travers le monde. Les moteurs de recherche généralistes, comme *Google Search*, sont alimentés ainsi.

L'univers des données collectées en ligne est encore bien plus vaste. Nous n'avons mentionné jusqu'ici que ce que M. Cardon appelle des « signaux ». Il s'agit de l'ensemble des « contenus explicites, informations ou expressions subjectives » : l'internaute livre activement des informations à un service ou à un interlocuteur, et il en a conscience. À ces signaux doivent être ajoutés des « traces », « enregistrements contextuels de comportements [...] (clics, géolocalisation, navigation, vitesse de lecture, etc.) »⁸⁵. Autrement dit, la manière même de naviguer sur Internet fait l'objet d'une recension très précise. Faire défiler une page Internet puis ralentir tout à coup face à un élément particulièrement intéressant, avant de reprendre un défilement plus rapide, cela revient souvent à produire une information, qui pourra être exploitée à des fins publicitaires notamment. L'internaute n'a pourtant rien exprimé, et n'a peut-être pas même eu conscience de ce comportement. De même saura-t-on qu'il s'est connecté à telle page mais, n'appréciant pas son premier coup d'œil, l'a quittée moins de quatre secondes plus tard ; qu'il y est toutefois revenu après qu'une publicité ciblée affichée sur le site de son quotidien préféré l'y aura incité ; qu'il y sera revenu une troisième fois le lendemain après réception d'un email « personnalisé » lui proposant un rabais exceptionnel de 10%, et aura finalement contracté.

51. Sur les traces de l'internaute : IP et cookies - Le premier vecteur de ces pratiques de suivi de l'internaute (*web tracking*) est l'adresse IP. Rappelons qu'il s'agit d'un identifiant chiffré, qui désigne un point d'accès au réseau ouvert par un fournisseur d'accès à Internet (FAI) ou plus précisément encore une machine connectée. Seul le FAI sait à quel client abonné correspond l'adresse IP. Même s'il est requis par les autorités, il ne pourra que leur fournir le nom de cet abonné, et pas le nom de la personne assise derrière l'écran. Or, il pourrait ne pas s'agir de la même personne dans le cas d'un point d'accès collectif (famille, association, entreprise, cybercafé). L'internaute réel pourrait même être un pirate ayant réussi à s'introduire dans le réseau wifi

84. - D. Cardon, *À quoi rêvent les algorithmes ? Nos vies à l'heure des big data*, Seuil, 2015, p. 11.

85. - *Ibid.*, p. 62.

d'autrui. En d'autres termes, même pour les pouvoirs publics s'étant adjoint le concours des FAI, l'adresse IP n'est pas totalement identifiante. Pour cette raison, la loi dite HADOPI a recouru à un expédient. Si une adresse IP est détectée sur un réseau de pair-à-pair, en train d'échanger des fichiers en violation du droit d'auteur, l'abonné n'est pas directement sanctionné pour contrefaçon - faute de preuve qu'il était bien au clavier - mais pour n'avoir pas suffisamment surveillé son point d'accès à Internet⁸⁶. Lorsqu'une plateforme observe qu'une requête lui est adressée par une certaine adresse IP, elle dispose de moins d'informations encore, puisqu'elle n'a pas accès au répertoire du FAI. Pourtant, cette information est extrêmement précieuse, pour deux raisons. La première raison est que l'adresse IP est porteuse d'une localisation géographique. Les adresses IP sont attribuées par l'*Internet Assigned Numbers Authority* (IANA), une branche de l'*Internet Corporation for Assigned Names and Numbers* (ICANN), la puissante association de droit californien qui gère les adresses Internet⁸⁷. La répartition des adresses IP n'a rien d'aléatoire. Une tranche d'adresses correspond à une fraction de territoire, d'une précision généralement au moins égale à la ville ou au village d'où se connecte l'internaute. L'adresse IP permet donc de savoir, avec une acuité relativement élevée, d'où se connecte un terminal lorsqu'il n'est pas possible d'obtenir une géolocalisation parfaite à l'aide d'une puce GPS. La deuxième raison pour laquelle l'adresse IP est précieuse, c'est qu'elle reste stable sur plusieurs jours, voire plus longtemps encore. Elle permet donc à un site de « reconnaître » un internaute qui n'en est pas à sa première visite. Elle constituera un substrat autour duquel vont s'agglomérer des informations, un embryon d'identité numérique, qui finira souvent par être rattaché à une identité stable. À elle seule, toutefois, l'adresse IP ne suffit pas à suivre, à tracer correctement les internautes. Le recours à des *cookies* est indispensable.

Pour expliquer ce qu'est un cookie, M. Lessig rappelle qu'aux origines d'Internet, les serveurs se contentaient de répondre aux requêtes des machines clientes (celles des visiteurs du site) sans rien savoir de ces machines. La page demandée était-elle la première consultée sur le site, ou y en avait-il eu une autre avant ? Si oui, laquelle ? Le serveur, incapable de faire un lien entre les différentes étapes d'une même session de navigation, était *a fortiori* inapte à reconnaître un visiteur au fil de ses différentes visites, sur des jours ou des semaines. Cette situation présentait certes d'importants

86. - Art. L. 336-3 al. 1 CPI : « La personne titulaire de l'accès à des services de communication au public en ligne a l'obligation de veiller à ce que cet accès ne fasse pas l'objet d'une utilisation à des fins de reproduction, de représentation, de mise à disposition ou de communication au public d'œuvres ou d'objets protégés par un droit d'auteur ou par un droit voisin sans l'autorisation des titulaires des droits prévus aux livres Ier et II lorsqu'elle est requise ». Ce texte est issu de la loi n° 2009-669 du 12 juin 2009 favorisant la diffusion et la protection de la création sur Internet, et a été modifié par la loi n° 2009-1311 du 28 octobre 2009 relative à la protection pénale de la propriété littéraire et artistique sur Internet à la suite d'une décision du Conseil constitutionnel présentée infra, n°119.

87. - V.infra, n°200.

avantages sur le plan de la préservation des vies privées, mais interdisait certaines fonctionnalités aujourd'hui considérées comme fondamentales :

Say you go to Amazon.com and indicate you want to buy 20 copies of my latest book. (Try it. It's fun.) Now your "shopping cart" has 20 copies of my book. You then click on the icon to check out, and you notice your shopping cart is empty. Why? Well because, as originally architected, the Web had no easy way to recognize that you were the same entity that just ordered 20 books. Or put differently, the web server would simply forget you. The Web as originally built had no way to remember you from one page to another. And thus, the Web as originally built would not be of much use to commerce. [...] But as I've said again and again, the way the Web was is not the way the Web had to be. And so those who were building the infrastructure of the Web quickly began to think through how the web could be "improved" to make it easy for commerce to happen. "Cookies" were the solution. In 1994, Netscape introduced a protocol to make it possible for a web server to deposit a small bit of data on your computer when you accessed that server. That small bit of data—the "cookie"—made it possible for the server to recognize you when you traveled to a different page.

En ce qu'il constitue la mémoire à long terme des serveurs, le *cookie* est devenu indispensable⁸⁸. Outre l'exemple du commerce électronique, on peut citer tous les services en ligne qui délivrent des contenus particuliers à la suite d'une authentification. Le *cookie* n'est donc pas une technique condamnable en soi. Mais une fois son principe admis, elle peut servir à enregistrer les plus infimes détails de la navigation, chaque clic de souris. « *Imagine libraries kept records of every time you opened a book at the library, even for just a second* »⁸⁹. Sur le moyen terme, non seulement un pool d'informations potentiellement très intimes a-t-il été constitué, mais il est presque certain qu'il pourra être rattaché à une identité stable. M. Lessig donne l'exemple d'un internaute qui, une seule fois, participe à un jeu-concours pour l'organisation duquel le site Internet demande les nom, prénom, adresse du joueur. Si le *cookie* n'est pas supprimé, il n'oubliera plus ces informations, qui flotteront en quelque sorte autour du pointeur de la souris à chaque future visite⁹⁰. Inquiétantes à l'échelle d'un site unique, ces techniques effraient lorsque l'on découvre qu'elles sont mises en œuvre, de manière croisée et collaborative, par de nombreux sites œuvrant en réseau. Car un site A peut fort bien héberger sur sa page des *cookies* qui ne sont pas fournis par lui, mais par ses partenaires X, Y, Z, qui sont souvent des régies publicitaires en ligne. Ces régies sont peu nombreuses, et sont présentes sur la grande majorité des sites visités par le grand public. Ainsi,

88. - Il existe une autre méthode d'authentification, dite par *token* (jeton) : elle consiste à intégrer les informations propres à l'internaute directement dans la requête envoyée au serveur. Concrètement, l'adresse internet du service est complétée par une chaîne de caractères unique, qui permet au serveur d'en savoir davantage sur la personne qui cherche à accéder à ses contenus. Par exemple, un utilisateur qui perd son mot de passe reçoit dans sa boîte mail un *token* sous forme de lien à usage unique : dans la requête figure un code qui indique au serveur que l'utilisateur est légitime. Toutefois, la méthode par jeton ne fonctionne qu'à l'échelle d'une session de navigation : elle est une mémoire à court terme, et ne remplace donc pas le *cookie*.

89. - L. Lessig, *Loc. cit.*

90. - *Ibid.*, p. 49.

compléter un formulaire nominatif sur n'importe laquelle des pages contractant avec ces régies revient à donner son identité à l'ensemble des membres du partenariat. En particulier, certains réseaux sociaux collaborent avec ces professionnels de la publicité en ligne. Or, aucun utilisateur d'un réseau comme Facebook ne peut prétendre rester anonyme, quand bien même il se serait inscrit sous un pseudonyme⁹¹.

Les moyens permettant de tracer les activités en ligne sont donc aujourd'hui d'une très grande puissance. Mais la récolte d'informations hors-ligne est tout aussi importante.

52. Les informations recensées par les téléphones intelligents - Les frontières de la présence en ligne et hors-ligne sont devenues particulièrement poreuses depuis la généralisation des téléphones intelligents. Chaque utilisateur d'un appareil de ce type est, en quelque sorte, connecté en permanence. Mais il est important de relever que ces appareils fournissent des données à des tiers même lorsque leur propriétaire n'est pas en train d'utiliser un service en ligne. En effet, même s'ils comportent des navigateurs classiques permettant de visiter des sites Internet — et qui recueillent des cookies —, ces téléphones intelligents reposent surtout sur des applications, choisies par le propriétaire du terminal pour lui rendre service. Ces applications requièrent, lors de leur installation, un accès plus ou moins étendu aux différentes couches d'information du système d'exploitation. Ainsi, une application d'aide à la navigation automobile demandera accès à la géolocalisation. Une application de messagerie sollicitera une autorisation d'accéder aux données concernant les contacts de l'utilisateur. Ce système se raffine au fur et à mesure des évolutions des principaux systèmes d'exploitation sur mobile — notamment iOS d'Apple et Android de Google — mais il était au départ très grossier : les catégories d'utilisation étaient très larges, l'utilisateur était peu informé. Surtout, une fois l'autorisation accordée, elle peut être utilisée en permanence. L'application de messagerie peut scruter la composition du carnet d'adresses, la durée et la destination des appels... alors même que cela n'est probablement pas strictement nécessaire au service. L'application de navigation peut demander sans cesse où se trouve le terminal, alors même qu'aucune aide à la conduite n'est en cours. La CNIL et l'INRIA, après avoir procédé à une batterie de tests, relèvent par exemple :

Ainsi, une application de service de réseau social a pu accéder 150 000 fois en 3 mois à la localisation d'un de nos testeurs. Cela représente un accès en moyenne par minute. Certaines applications qui ont obtenu l'autorisation (générique) d'accéder à la localisation ne se privent donc pas de l'utiliser, même lorsque l'application n'est pas visible à l'écran. D'une manière générale, beaucoup d'applications accèdent très souvent à la localisation (ainsi, plus de 3 000 fois en 3 mois pour un jeu). En volume, la

91. - P. Eckersley, « How online tracking companies know most of what you do online (and what social networks are doing to help them) », article *eff.org* du 21/09/09.

géolocalisation est aussi la donnée la plus collectée : elle représente à elle seule plus de 30% des événements détectés, sans être toujours liée à des fonctionnalités offertes par l'application ou à une action de l'utilisateur⁹².

53. Les objets connectés - Les frontières des mondes en ligne et hors-ligne se brouillent encore lorsque l'on évoque les objets connectés, qui visent précisément à rattacher les choses du quotidien au réseau⁹³. Cela permet leur pilotage à distance, soit par leur propriétaire situé n'importe où dans le monde, à l'aide d'un terminal, soit par des algorithmes censés les rendre « intelligents ». Objets connectés, avez-vous donc une âme ? Ainsi un thermostat connecté permet-il à une famille rentrant de vacances plus tôt que prévu de rallumer la chaudière à distance, afin que la maison soit à la température souhaitée en arrivant. Mais il peut, le reste du temps, être dirigé par un algorithme qui tiendra compte des prévisions météorologiques et des caractéristiques du logement pour piloter plus finement les variations dans la puissance de chauffage. Il en résulterait des économies d'énergie⁹⁴. Puisque « l'intelligence » de l'objet n'est pas logée dans un processus implanté localement, mais à distance, il devient « nécessaire » de fournir aux serveurs de l'entreprise le commercialisant un ensemble de données très précieuses sur les habitudes du foyer. Le relevé et la transmission des consommations du foyer peut être la finalité principale de l'objet connecté : c'est le cas des compteurs intelligents, comme le Linky d'Enedis. Parfois, l'objet aura pour mission de passer des commandes à un commerce en ligne pour le compte de son propriétaire⁹⁵. Parfois encore, son accès au réseau lui servira à diffuser des contenus : c'est le cas des téléviseurs connectés. Ces derniers ont parfaitement illustré le risque présenté par les objets connectés. La *Federal Trade Commission* américaine vient d'infliger une amende supérieure à 2 millions de dollars à un fabricant de téléviseurs connectés qui espionnaient ses utilisateurs, à leur insu, en analysant seconde après seconde les contenus diffusés sur son écran. Ces données étaient croisées avec celles récoltées par des tiers afin de connaître le sexe, l'âge, les revenus, le statut familial, ou encore le niveau d'éducation des occupants⁹⁶.

92. - CNIL, *Mobilitics, saison 2 : nouvelle plongée dans l'univers des smartphones et de leurs applications*, publication cnil.fr du 15/12/14.

93. - G. Haas, A. Dubarry, M. D'auvergne et R. Ruimy, « Enjeux et réalités juridiques des objets connectés », *Dalloz IP/IT*, 2016, p. 394 ; E. Geffray, « Quelle protection des données personnelles dans l'univers de la robotique ? », *Dalloz IP/IT*, 2016, p. 295.

94. - Pour une description du produit le plus répandu sur le marché français : <https://www.netatmo.com/fr-FR/product/energy/thermostat>.

95. - Il peut s'agir d'un simple raccourci physique actionné par l'être humain, comme le *Dash Button* d'Amazon qui, d'une simple pression, reçoit instruction de commander un produit déterminé ; il peut s'agir d'une « initiative » de l'objet connecté comme ces réfrigérateurs supposés anticiper les besoins en alimentation de la famille, et capables d'y pourvoir de leur propre chef en passant les commandes adéquates.

96. - Federal Trade Commission, *VIZIO to pay \$2.2 million to FTC, state of new jersey to settle charges it collected viewing histories on 11 million smart televisions without users' consent*, publication ftc.gov du 6/02/17.

54. Les informations collectées hors-ligne - Même les personnes ne naviguant jamais sur Internet et ne disposant que d'un téléphone traditionnel ne sont pas à l'abri de cette grande moisson d'informations. Si l'individu n'est pas connecté, ses interlocuteurs privés et publics le sont. Les modes d'alimentation des bases de données sont multiples, et vont de la saisie manuelle par une administration ou un agent d'assurance jusqu'à l'emploi de cartes de fidélité, sans oublier les informations particulièrement sensibles et précises que constituent les données bancaires, résultant du fonctionnement des comptes et moyens de paiement.

Comme l'écrit un auteur, « les capteurs numériques sont en train de jeter leur filet sur le monde pour le rendre mesurable en tout. Le savoir et les connaissances, les photographies et les vidéos, nos mails et ce que nous racontons sur Internet, mais aussi nos clics, nos conversations, nos achats, notre corps, nos finances ou notre sommeil deviennent des données calculables »⁹⁷. Ces données ont ensuite vocation à être exploitées.

2 - Des traitements à grande échelle

55. Le traitement décorrélé de l'identité - Il est possible d'extirper une valeur aux données, qu'elle soit scientifique ou économique, en les détachant de toute identité stable. « *Big data* » : l'expression est à la mode. On peine à en trouver une définition précise, et elle semble relever davantage d'un discours marketing que d'un concept scientifique identifié. Elle renvoie simplement à l'étude d'un ensemble extrêmement volumineux de données⁹⁸. Une telle analyse peut être conduite selon des méthodes et pour la poursuite de finalités très diverses. Le secteur des assurances, par exemple, est accoutumé depuis longtemps à construire des prédictions de risques à partir de données nombreuses, tirées notamment des sinistres antérieurs. La démarche, en soi, n'est donc absolument pas nouvelle. Simplement, les sources de données sont, on l'a vu, devenues innombrables, et les capacités de traitement informatique ont explosé, ce qui augmente les capacités de projection des actuaires de ces compagnies.

Mais le *big data* renvoie aussi à des usages véritablement nouveaux. Il peut s'agir d'améliorer des infrastructures collectives, en identifiant les besoins pour mieux répartir les ressources. Les dizaines de milliers de circuits individuels parcourus par des automobilistes, et connus des logiciels de navigation GPS ou de l'entreprise de transport Uber peuvent être cédés à des villes, afin qu'elles améliorent leur réseau routier⁹⁹.

97. - D. Cardon, *op. cit.*, p. 8.

98. - V. par ex. L. Marino, « Notre vie privée : des little data aux big data », *JGP G*, 2012, n° 47.

99. - C. Durand, « Les données d'Uber sur la circulation, une mine d'or pour les villes et leurs urbanistes », article *Numerama.com* du 9/01/17.

Autre application du *big data*, l'apprentissage statistique (*machine learning*) permet aux ordinateurs d'acquérir de nouvelles compétences jusqu'ici réservées à l'être humain. Ainsi peuvent-ils reconnaître des objets ou des personnes sur des images, ou apprendre à conduire, après avoir analysé des millions de cas concrets puisés dans des réservoirs de données.

Dans ces exemples, il n'est pas nécessaire de continuer à associer une identité aux données personnelles. Peu importe qui étaient les 50 000 conducteurs qui ont parcouru la ville de Boston en transmettant leur géolocalisation, permettant d'améliorer ses infrastructures, ou enregistrant l'ensemble de leurs actions de conduite à des fins de *machine learning*. Parfois, il faut cependant connaître des caractéristiques de l'individu, théoriquement non identifiantes à elles seules, pour que les données puissent être employées : un assureur qui veut cerner un risque maladie doit savoir si les données proviennent d'un fumeur ; celui qui travaille sur le risque d'accident automobile souhaite connaître l'âge, l'ancienneté du permis, le type de véhicule, et même le sexe du conducteur¹⁰⁰.

L'analyse de données de masse peut servir à adapter des contenus publicitaires à un individu précis, sans nécessairement rechercher son identité stable. Grâce à des cookies répartis sur un ensemble de sites partenaires, une régie publicitaire connaît les sites consultés par un individu sur plusieurs semaines. Elle opère un rapprochement avec des profils similaires relevés chez des milliers d'autres personnes. L'algorithme relève que, parmi elles, nombreuses sont celles qui ont fait l'acquisition d'un bien de consommation particulier : une publicité pour cet objet s'affichera à son intention. Il n'est même pas nécessaire de passer par un *raisonnement* - de type : « *puisque* ces personnes s'intéressent aux nouvelles technologies, il faut *donc* leur proposer un téléphone dernier cri ». Une simple corrélation est aujourd'hui employée : « ceux qui ont visité les mêmes sites que lui ont ensuite acheté un téléphone dernier cri ». Dans cette hypothèse, la régie publicitaire n'a pas plongé dans l'identité numérique jusqu'à son noyau, l'identité stable. Elle s'est contentée de naviguer à la périphérie, au sein de signaux et de traces anonymes.

56. Le traitement corrélé à l'identité - Souvent, le traitement est bel et bien corrélé à l'identité. C'est évidemment le cas lorsque la personne elle-même fournit ses « coordonnées juridiques et sociales uniques » : un NIR, un ensemble constitué de ses nom, prénom, lieu et date de naissance... Mais au moins a-t-elle conscience, alors, que les données collectées dans ce cadre s'agglutineront

100. - Il n'est certes plus permis aux assureurs d'utiliser le critère du sexe pour le calcul de la prime réclamée à leurs assurés depuis un arrêt de la CJUE du 1er mars 2011, C-236/09, *Tests-Achats*. La décision est fondée sur les articles 21 et 23 de la Charte des droits fondamentaux. Cela n'empêche toutefois pas d'utiliser le sexe pour pondérer les risques, en interne, ou dans les relations entre assureurs et réassureurs. V. Commission européenne, *Lignes directrices sur l'application de la directive 2004/113/CE du Conseil dans le secteur des assurances, à la lumière de l'arrêt de la Cour de justice de l'Union européenne dans l'affaire C-236/09 (Test-Achats)*, texte 2012/C 11/01, JOUE.

autour de son identité stable. Le plus inquiétant n'est pas là : c'est la facilité avec laquelle, par un jeu de recoupements et de déduction, il est possible, et facile, de passer d'un jeu de données théoriquement anonyme à l'identité d'une personne unique. Une importante régie publicitaire en ligne présente ses méthodes comme suit : « Contrairement aux méthodes probabilistiques généralement proposées par les autres solutions publicitaires, Universal Match est une composante unique développée par Criteo qui permet de comprendre les intentions d'achats d'un individu à travers l'ensemble des appareils, navigateurs et applications, grâce à une identification anonyme de l'utilisateur »¹⁰¹. Cette « identification anonyme », aux allures d'oxymore, repose sur la substitution au nom d'un pseudonyme, constitué d'une suite de chiffres et de lettres sans signification apparente. Mais cela signifie bien que l'entreprise dispose, pour chaque individu, d'un et un seul répertoire de données. Au-delà des frontières apparentes que constituent les différents terminaux, les différentes localisations de l'individu, l'entreprise voit l'utilisateur - elle voit l'homme. D'un tel profil à la révélation de l'identité stable, il n'y aurait qu'un saut de puce à accomplir.

À quoi sert-il de corréler un ensemble de données à une identité ? On l'a vu, à améliorer encore les performances de la publicité ciblée par rapport à une approche statistique anonyme - un enjeu qui pèse des milliards. Cela peut encore servir à prendre des décisions lorsque l'individu concerné se présente à une banque ou à une compagnie d'assurance : contracter ou pas avec lui, et à quelles conditions. Cela peut servir à identifier un délinquant, à briser l'anonymat sous lequel il croyait agir.

Des années 70 à nos jours, nous avons assisté à la montée en puissance de l'avatar numérique de l'individu. Voyons à présent comment notre système juridique le protège.

Section 2 - La protection de l'identité numérique

57. Une accélération de la production normative - La constitution et le maniement de fichiers contenant des informations exsudées, en ligne et hors-ligne, par les personnes physiques, ont d'abord été encadrés par la loi précitée de 1978 dite « informatique et libertés »¹⁰².

Des textes nombreux ont ensuite été adoptés au niveau de l'Union européenne. Une directive a été adoptée en 1995, portant de manière générale sur la protection des données¹⁰³ ; elle a rendu

101. - <http://www.criteo.com/fr/products/>.

102. - Loi n° 78-17, précitée.

103. - Directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données.

nécessaire la modification de la loi « informatique et libertés » par une loi de 2004¹⁰⁴. En 2000, la Charte des droits fondamentaux de l'Union européenne a consacré, en son article 8, un « droit à la protection des données à caractère personnel »¹⁰⁵. Fut ensuite adoptée une série de directives sectorielles, portant sur les données personnelles employées dans le secteur des communications électroniques¹⁰⁶, ou sur les données relatives aux infractions pénales¹⁰⁷. En 2016, un règlement européen sur la protection des données (dit « RGPD ») a été adopté¹⁰⁸. Il est entré en vigueur le 25 mai 2018, remplaçant la directive de 1995 et, dans une large mesure, la loi informatique et libertés. Une loi française du 20 juin 2018 a exploité les nombreux espaces dans lesquels le RGPD laissait les États libres d'adopter une solution propre, tout en transposant en droit interne la directive relative aux infractions pénales¹⁰⁹. Enfin, au cours de l'année 2019, un autre règlement européen devrait remplacer les directives relatives au secteur des communications¹¹⁰.

104. - Loi n° 2004-801 du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et modifiant la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

105. - « 1) Toute personne a droit à la protection des données à caractère personnel la concernant. 2) Ces données doivent être traitées loyalement, à des fins déterminées et sur la base du consentement de la personne concernée ou en vertu d'un autre fondement légitime prévu par la loi. Toute personne a le droit d'accéder aux données collectées la concernant et d'en obtenir la rectification. 3) Le respect de ces règles est soumis au contrôle d'une autorité indépendante ».

106. - Directive 97/66/CE du Parlement européen et du Conseil du 15 décembre 1997 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des télécommunications ; directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive vie privée et communications électroniques) ; directive 2006/24/CE du Parlement européen et du Conseil du 15 mars 2006 sur la conservation de données générées ou traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public ou de réseaux publics de communications, et modifiant la directive 2002/58/CE.

107. - Directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil.

108. - Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données) (Texte présentant de l'intérêt pour l'EEE).

109. - Loi n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles, sur laquelle V. la décision de non conformité partielle du Conseil constitutionnel, n° 2018-765 DC du 12 juin 2018. Cette loi habilite le Gouvernement à réécrire le droit français des données personnelles sous la forme d'une ordonnance plus lisible. Ce texte n'est pas encore disponible au moment où nous écrivons.

110. - Proposition de règlement du Parlement européen et du Conseil concernant le respect de la vie privée et la protection des données à caractère personnel dans les communications électroniques et abrogeant la directive 2002/58/CE (règlement «vie privée et communications électroniques»), 2017/0003 (COD).

Dans l'intervalle, en droit interne, d'autres lois générales et sectorielles ont comporté des dispositions intéressant les informations personnelles¹¹¹.

Les textes précités, notamment la loi « informatique et libertés » et le règlement de 2016, s'appliquent en présence d'informations d'une certaine nature, et uniquement lorsque certains traitements sont appliqués à ces informations. Voyons comment sont définis ces concepts-clés.

58. Quelles informations ? - En 1978, la loi visait les « informations nominatives », étant aussitôt précisé : « sont réputées nominatives au sens de la présente loi les informations qui permettent, sous quelque forme que ce soit, **directement ou non, l'identification** des personnes physiques auxquelles elles s'appliquent [...] »¹¹². Il s'agit donc bien de protéger l'identité (stable) des personnes physiques, en prenant dans les filets de cette législation toute information susceptible d'y être rattachée, y compris de la manière la plus indirecte. Aucun passage par le nom n'est véritablement nécessaire : un fichier recensant une profession rattachée à un numéro RIN pointe vers un et un seul individu ; que l'on puisse ensuite redescendre de son identité stable à son nom est à la fois évident et secondaire. Aussi faut-il se féliciter de ce que la directive de 1995 ait repoussé l'expression « informations nominatives » au profit de « données à caractère personnel ».¹¹³ La définition retenue est cette fois-ci : « [...] toute information concernant une personne physique identifiée ou identifiable [...] directement ou indirectement »¹¹⁴. On la retrouve dans le règlement de 2016¹¹⁵. La forme prise par l'information importe peu : textes, sons, images, données biométriques peuvent être concernés. Elle doit se rapporter à une personne physique vivante - les morts et les personnes morales ne sont pas concernés¹¹⁶.

111. - Notamment la loi du 26 janvier 2016 n° 2016-41 de modernisation de notre système de santé et la loi n° 2016-1321 du 7 octobre 2016 pour une République numérique.

112. - Article 4 de la loi n° 78-17 dans sa version d'origine. Souligné par nous.

113. - Directive 95/46/CE précitée, qui emploie cette expression dans son intitulé même ; art. 2 de la loi du 6 janv. 1978 tel que modifiée par la loi n° 2004-801.

114. - Art. 1er : « Aux fins de la présente directive, on entend par : a) “données à caractère personnel” : toute information concernant une personne physique identifiée ou identifiable (personne concernée) ; est réputée identifiable une personne qui peut être identifiée, directement ou indirectement, notamment par référence à un numéro d'identification ou à un ou plusieurs éléments spécifiques, propres à son identité physique, physiologique, psychique, économique, culturelle ou sociale ; [...] ». Pour une étude approfondie cherchant à distinguer « informations nominatives » et « données à caractère personnel » : J. Eynard, *Les données personnelles. Quelle définition pour un régime de protection efficace ?*, éd. Michalon, 2013.

115. - Article 4 du règlement 2016/679 précité. On se contente d'ajouter des exemples de moyens d'identification : données de localisation, identifiant en ligne.

116. - F. Lesaulnier, « La définition des données à caractère personnel dans le règlement général relatif à la protection des données personnelles », *Dalloz IP/IT*, 2016, p. 573. L'éviction des défauts du champ d'application résulte du considérant 27 du règlement ; celle des personnes morales, du considérant 14.

Puisqu'il suffit que l'information permette « indirectement » l'identification d'une personne, le champ des données concernées est très vaste. L'adresse IP en constitue un bon exemple. Il a déjà été exposé que cette adresse désigne non pas un individu, mais un point d'accès au réseau ou au mieux, une machine connectée au réseau¹¹⁷. Pour cette raison, la Chambre criminelle de la Cour de cassation avait jugé que l'adresse IP, collectée par un agent assermenté traquant des violations du droit d'auteur sur les réseaux de pair-à-pair, n'était pas une donnée personnelle¹¹⁸. Récemment, la Première chambre civile a jugé tout au contraire, de manière parfaitement convaincante, que « les adresses IP, qui permettent d'identifier **indirectement** une personne physique, sont des données à caractère personnel »¹¹⁹. La CJUE va dans le même sens, expliquant que des voies de droit existent en Allemagne — pays concerné par cet arrêt — pour obtenir du fournisseur d'accès à Internet le nom de l'abonné correspondant à une adresse IP¹²⁰. Et il est vrai que connaître le nom de l'abonné permet de connaître le nom de l'internaute lorsqu'une seule personne utilise le point de connexion au réseau ou la machine - ce qui emporte déjà la décision. Même lorsque plusieurs personnes utilisent la même adresse IP, la combiner avec d'autres informations — par exemple les autres sites visités par la même IP durant une certaine tranche horaire — permettent très souvent de déduire qui du père, de la mère ou des enfants, par exemple, se trouvait au clavier.

Il est donc fondamental de considérer non seulement ce que dit déjà un jeu de données personnelles donné lorsqu'on le contemple, mais aussi et surtout ce qu'il pourrait dire s'il était croisé ou combiné avec d'autres informations. C'est aussi pour cette raison que le règlement s'applique également aux données qui n'ont pas été totalement « anonymisées », mais seulement « pseudonymisées » : même si les noms ont été transformés en codes *a priori* incompréhensibles, dès lors qu'il existe une possibilité de remonter jusqu'à l'identité d'une personne par des moyens indirects, des déductions, des recoupements, le régime applicable est celui des données personnelles¹²¹. Dans ces conditions, la question se pose de savoir si les données véritablement

117. - V. *supra*, n°51.

118. - Cass. crim., 13 janv. 2009, n° 08-84.088. Plus précisément, la Cour juge que la collecte des adresses IP ne constitue pas « un traitement de données à caractère personnel [...] ». Cela revient implicitement, mais nécessairement à affirmer que l'IP n'est pas une donnée à caractère personnel.

119. - Cass. 1ère civ., 3 nov. 2016, n° 15-22.595. Souligné par nous. La CNIL avait déjà décidé en ce sens, par exemple dans sa délibération n° 2013-420 de la formation restreinte prononçant une sanction pécuniaire à l'entre de la société Google Inc.

120. - CJUE, 19 oct. 2016, C-582/14. La décision portait de surcroît sur des adresses IP dynamiques, c'est-à-dire renouvelées à chaque nouvelle connexion de l'abonné au réseau, qui sont moins facilement identifiantes que des adresses statiques.

121. - Considérant 26 du règlement précité : « Les données à caractère personnel qui ont fait l'objet d'une pseudonymisation et qui pourraient être attribuées à une personne physique par le recours à des informations supplémentaires devraient être considérées comme des informations concernant une personne physique identifiable ». Sur cette question, V. F. Lesaulnier, art. préc. ; R. Perray et J. Uzan-Naulin, « Existe-t-il encore des

anonymes existent : un chercheur a montré qu'en croisant trois informations banales et d'apparence inoffensive — le sexe, le code postal et la date de naissance — on parvient à identifier de manière unique 63% de la population américaine¹²² !

59. Quelles opérations ? - Les textes sont applicables à certains usages des données ainsi caractérisées. Le règlement les appelle « traitement(s) de données à caractère personnel » et les définit comme « toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données ou des ensembles de données à caractère personnel, telles que la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation, l'effacement ou la destruction »¹²³. La liste est d'une étendue telle qu'on imagine mal une opération intellectuelle, physique, scientifique ou commerciale sur des données qui ne s'y trouverait pas. Il faut relever que même les manipulations non automatisées de données sont concernées, de sorte que des fichiers papier, par exemple, sont concernés par le texte - ils sont certes devenus rares¹²⁴.

60. Quelle articulation avec le droit à la vie privée ? - Peut-on considérer les « règles relatives à la protection des personnes physiques à l'égard du traitement des données à caractère personnel »¹²⁵ comme un nouveau visage du droit à la vie privée, à l'ère numérique ? Les notions ne se confondent pas, mais il est vrai qu'elles entretiennent des liens indéniables et puissants.

données non personnelles ? », *Dalloz IP/IT*, 2017, p. 286.

122. - P. Golle, « Revisiting the uniqueness of simple demographics in the US population » : <https://crypto.stanford.edu/~pgolle/papers/census.pdf>. Ce chercheur revoit à la baisse le chiffre de 87% qui avait été avancé par Mme Latanya Sweeney dans un projet d'article qui, quoique non publié, avait été repris par plusieurs grands médias, par exemple S. Schoen, « What information is "personally identifiable" », article du 11/09/11 : <https://www.eff.org/deeplinks/2009/09/what-information-personally-identifiable>. Le chiffre reste considérable.

123. - Article 2 b) du règlement 2016/679 précité.

124. - La loi informatique et libertés de 78 ne visait que les traitements automatisés, ce qui a fait l'objet d'un débat devant l'Assemblée nationale. Le garde des sceaux Alain Peyrefitte expliquait ainsi sa position : « qui trop embrasse, mal étreint. Les fichiers manuels sont extrêmement nombreux : de par le côté artisanal de leur utilisation, ils présentent en réalité peu de dangers pour les libertés, car le recoupement des informations — et c'est cela qui est dangereux et crée un risque — est presque impossible en raison de la lenteur des manutentions : les interconnexions entre fichiers manuels sont tellement malcommodes qu'elle ne sont pas à craindre. Un argument encore plus décisif va dans le même sens : si la commission devait s'occuper à la fois des fichiers informatiques — et elle attrait déjà beaucoup à faire avec ceux-ci — et des fichiers manuels, il est clair qu'elle n'aurait le temps de s'occuper ni des uns ni des autres. Mieux vaut donc s'occuper de ce qui en vaut la peine » (compte-rendu de la séance du 4 octobre 1977, JO, p. 5789).

125. - Art. 1, 1 du règlement 2016/679 précité.

M. Gutmann qualifie la vie privée de « zone soustraite au regard » et rappelle qu'historiquement, cette zone devait s'entendre littéralement, comme un espace physique. « La dimension matérielle de l'espace privé ne doit rien au hasard : alors que le Code civil clôturait soigneusement les espaces privés, l'histoire récente de la vie privée fait bien apparaître le lien intime entre le développement de cette notion et l'augmentation de la taille des logements urbains qui a permis aux individus, au sein de leur famille, d'acquérir un espace propre »¹²⁶. Mais l'auteur avertit que cette notion a évolué, pour désigner par la suite un espace avant tout immatériel. Ainsi, appliquant l'article 368 du Code pénal, qui sanctionnait les enregistrements et photographies réalisés dans un lieu privé, « certains juges avaient introduit dans l'appréciation de ce lieu un élément subjectif, permettant de protéger ceux qui, quoique placés dans un espace public, avaient entendu soustraire aux regards importuns des éléments de leur vie privée »¹²⁷.

De manière similaire, M. Lessig explique comment le droit américain a évolué dans son interprétation du 4ème amendement à la Constitution des États-Unis, qui protège les citoyens contre les intrusions injustifiées des pouvoirs publics¹²⁸. Ce texte a d'abord été interprété en 1928 comme ne s'appliquant pas à un dispositif de mise sur écoute placée sur une ligne téléphonique, si le tronçon de ligne manipulé par les autorités se trouvait dans un endroit public, et qu'il n'a donc pas été nécessaire de pénétrer sur la propriété privée de la personne surveillée¹²⁹. Ce n'est qu'en 1967 qu'une conception plus immatérielle de la vie privée a conduit à renverser cette solution¹³⁰.

Comment définir cette vie privée moderne et immatérielle ? M. Gutmann propose d'y voir « un ensemble d'informations personnelles », mais met aussitôt en garde contre une assimilation avec les données à caractère personnel au sens de la directive de 1995¹³¹. En effet, on trouve parmi les données à caractère personnel aussi bien des informations privées que publiques¹³². Un titre

126. - D. Gutmann, *op. cit.*, p. 216.

127. - *Ibid.*, p. 217. L'auteur se réfère à l'affaire Romy Schneider. L'actrice se trouvait sur un navire, au large, sans autre navire visible au loin. Elle se trouvait donc dans un espace théoriquement public, mais qui semblait présenter toutes les garanties d'intimité, de sorte que la vie privée devait y être protégée aussi bien qu'au sein d'un domicile (CA Paris, 5 févr. 1979, JCP 1980, II, 19343, note R. Lindon).

128. - « *The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized* ».

129. - « *The tapping connections were made in the basement of a large office building and on public streets, and no trespass was committed upon any property of the defendants. Held, that the obtaining of the evidence and its use at the trial did not violate the Fourth Amendment* ». *Olmstead v. United States*, 277 U.S. 438 (1928), commenté par L. Lessig., *Code V.2, op. cit.*, p. 157 s.

130. - *Katz v. United States*, 389 U.S. 347 (1967).

131. - D. Gutmann, *op. cit.*, p. 228, note 27.

132. - J. Eynard, *op. cit.*, spéc. p. 63 s.

professionnel, des informations sur la filiation de l'individu consultables à l'état civil sont des données personnelles, mais non des informations relatives à la vie privée.

Les notions sont donc distinctes, mais pas étrangères l'une à l'autre. La directive de 1995 affirmait : « l'objet des législations nationales relatives au traitement des données à caractère personnel est d'assurer le respect des droits et libertés fondamentaux, notamment du droit à la vie privée reconnu également dans l'article 8 de la convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales et dans les principes généraux du droit communautaire »¹³³. En droit interne, dès 1978, la loi informatique et libertés s'ouvrait sur cette proclamation : « L'informatique doit être au service de chaque citoyen. Elle ne doit porter atteinte ni à l'identité humaine, ni aux droits de l'homme, ni à la vie privée, ni aux libertés individuelles ou publiques »¹³⁴.

L'encadrement des données personnelles aurait donc vocation à renforcer, à soutenir le droit à la vie privée. Cette présentation est cohérente. Les données personnelles comprennent toutes les informations relatives à la vie privée, et d'autres encore. La relation entre ces deux ensembles est donc celle du genre à l'espèce. Mais à quoi sert-il de protéger l'autre espèce, les données publiques ? Pourquoi réglementer la constitution et la manipulation de fichiers contenant des informations qui devraient être librement accessibles à chacun ? Le critère déclenchant l'application du droit des données personnelles doit être le plus clair et le plus durable possible, quitte à être très large. La notion de vie privée varie de manière significative dans le temps et dans l'espace. Lorsqu'une personne prétend qu'il a été porté atteinte à sa vie privée, un débat judiciaire s'instaure et ce n'est finalement qu'au dénouement du procès que l'on sait si la vie privée était bien en cause¹³⁵. Le droit des données personnelles, qui prétend s'appliquer à toute personne qui manipule du bout du doigt une information relative à un individu identifiable, ne pourrait s'accommoder de telles incertitudes. Le critère de l'information susceptible d'être rattachée à une personne est d'un maniement plus aisé¹³⁶.

En somme, le droit à la vie privée est un pouvoir d'exclure autrui d'une sphère restreinte d'intimité, généralement invoqué lorsque la menace est déjà tangible. Le droit à la protection des données à caractère personnel concerne très largement toute information susceptible d'être

133. - Considérant n° 10 de la directive 95/46/CE précitée.

134. - Art. 1er, al. 1 de la loi n° 78-17 précitée. Cet alinéa est toujours libellé ainsi en droit positif.

135. - « À l'évidence, la substance de la vie privée est dépendante des pratiques et des discours, des "mœurs" en vigueur à un moment donné dans la société, dont les juges se font la voix instantanée — donc incomplète ou infidèle — et toujours provisoire » (D. Gutmann, *op. cit.*, n° 261).

136. - Nous avons vu cependant que ses frontières ne sont pas parfaitement stables : au fur et à mesure que les techniques mathématiques d'analyse des informations se perfectionnent, le champ des données qui doivent être qualifiées comme personnelles augmente : V.*supra*, n°58.

rattachée, même indirectement, à un individu donné ; il a une visée essentiellement préventive plutôt que curative, en posant *a priori* dans quel cadre et à quelles conditions les informations peuvent être exploitées. Ainsi, pour caractériser la relation qui unit les concepts, il est tentant de paraphraser la célèbre formule de Ihéring sur la possession, et de présenter le droit des données personnelles comme le bastion avancé de la vie privée à l'ère numérique¹³⁷.

61. À qui incombe la protection ? - Il n'est pas question, dans les développements qui vont suivre, de décrire en détail un droit foisonnant et technique, auquel des traités sont exclusivement consacrés¹³⁸. Il s'agira d'une présentation des lignes de force, qui permettra de mieux comprendre comment se forme l'identité numérique des personnes aujourd'hui, et comment elle est protégée par le droit. Précisons par ailleurs qu'il ne sera pas traité de l'arsenal législatif antiterroriste, qui réduit la vie privée des citoyens pris dans son champ d'application à la portion congrue : ses logiques spécifiques appelleront une présentation séparée, dans une version ultérieure de cette étude¹³⁹.

Deux points de vue pourraient être défendus. L'un consisterait à dire que les individus sont incapables — par manque de compétence, de temps, et peut-être d'intérêt — de défendre eux-mêmes leur identité numérique. Une telle analyse doit conduire à un droit des données à caractère personnel protecteur, dirigiste, impératif. Le second point de vue voudrait qu'on laisse aux personnes concernées le soin de fixer elles-mêmes ce qui constitue un usage acceptable des informations qu'elles cèdent ou sèment derrière elles. La réglementation serait alors libérale, souple, personnalisée.

Le droit positif ne choisit pas entre ces deux approches, mais les combine. D'abord, nombre de règles s'imposent à ceux qui décident de manipuler les données : les « responsables de traitement »¹⁴⁰, ainsi qu'à leurs sous-traitants et partenaires. Ensuite, des moyens juridiques et

137. - Il a déjà été précisé que le droit des données personnelles s'applique aux fichiers non numériques. Mais ceux-ci sont en voie de disparition, et ne constituent pas la menace la plus tangible.

138. - Notamment A. Debet, J. Massot et N. Metallinos (ss. la dir.), *Informatique et libertés. La protection des données à caractère personnel en droit français et européen*, Lextenso, 2015.

139. - À titre de simple exemple, le projet de loi renforçant la sécurité intérieure et la lutte contre le terrorisme, adopté par l'Assemblée nationale le 3 octobre 2017, prévoit en son article 3 que le ministre de l'intérieur peut forcer toute personne soupçonnée d'entretenir des liens avec le terrorisme à « [...] déclarer les numéros d'abonnement et identifiants techniques de tout moyen de communication électronique dont elle dispose ou qu'elle utilise [...] », sous peine de se voir infliger une peine de trois ans d'emprisonnement et 45 000 euros d'amende.

140. - L'art. 4 du règlement UE 2016/679 précité définit comme « “responsable du traitement”, la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement », étant précisé que « lorsque les finalités et les moyens de ce traitement sont déterminés par le droit de l'Union ou le droit d'un État membre, le responsable du traitement peut être désigné ou les critères spécifiques applicables à sa désignation peuvent être prévus par le droit de l'Union ou par le droit d'un État membre ».

techniques s'offrent aux individus eux-mêmes afin de contrôler, préserver, modeler leur identité numérique. Ils supposent de leur part une prise de conscience de cette identité, puis une allocation de temps et d'énergie pour comprendre et mettre en œuvre les outils permettant de la façonner.

Il est alors utile de présenter séparément ces deux corps de règles. Dans la situation — courante — où les individus dont les données sont exploitées se désintéressent de la question, le statut impératif des responsables de traitement donne à voir les seules garanties qui seront mises en œuvre, la protection plancher (I). Mais dans les cas où les individus se préoccupent de la consistance et des usages de leurs données, il est bon de consacrer une étude distincte à l'ensemble d'outils qui s'offrent à eux afin de gérer le plus finement possible leur identité numérique (II).

I - La protection plancher exigée des responsables de traitement

62. **Plan** - Les textes de droit interne et de droit européen forment un entrelacs complexe dont nous ne retiendrons que l'essentiel. Il faudra présenter la collecte (A), l'exploitation (B) et la circulation (C) des données à caractère personnel, ainsi que les sanctions susceptibles d'être prononcées si ces règles ne sont pas respectées (D). Précisons d'emblée qu'une grande partie des obligations qui incombent aux responsables de traitement pèse également sur les sous-traitants qu'ils décideraient de faire intervenir : nous y reviendrons.

A - La collecte des données

63. **Une collecte sobre et finalisée** - Parmi les grands principes qui régissent les opérations sur données personnelles, l'une des règles centrales est celle-ci : « les données à caractère personnel doivent être [...] collectées pour des finalités déterminées, explicites et légitimes [...] »¹⁴¹. Il n'y a là aucune évidence. À l'ère du *big data*, il est tentant pour un opérateur d'attraper toutes les données qui passent à sa portée, en renvoyant à plus tard la question de leur utilisation¹⁴². Il faut au contraire qu'il détermine *a priori* les raisons pour lesquelles il souhaite procéder à la collecte, et qu'il se plie ensuite à une exigence de sobriété : les données doivent être « adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées (minimisation des données) »¹⁴³.

141. - Art. 5, b) du règlement UE 2016/679 précité.

142. - Intervention de M. P. Michel au colloque « le droit des données personnelles », Amiens, 7 novembre 2016.

143. - Art. 5, c) du règlement UE 2016/679 précité.

Un exemple concret permettra de mieux comprendre l'exigence cardinale de minimisation des données. S'il est possible au conducteur d'une « automobile connectée » d'obtenir, sur son tableau de bord, une estimation du temps qu'il fera là où il se trouve, la CNIL rappelle que l'application de météo n'a besoin ni d'une géolocalisation fine (à quelques mètres près), ni d'un accès permanent (toutes les secondes par exemple) à la position du véhicule dans l'espace¹⁴⁴. Il suffira d'une géolocalisation grossière (par exemple, à 1 kilomètre près) et d'un accès sporadique (toutes les 10 minutes), le tout étant traité en temps réel sans stockage durable de ces données.

De cette exigence de tempérance à la réalité des pratiques, il est à craindre qu'existe un gouffre. Il suffira de rappeler l'exemple déjà cité du réseau social ayant accédé 150 000 fois en trois mois à la géolocalisation d'un utilisateur : on ne voit pas quelle finalité (légitime) pourrait justifier un tel appétit¹⁴⁵. Cela pose naturellement la question des moyens dont disposent les autorités chargées des contrôles, sur les plans technique, budgétaire et sur celui des sanctions¹⁴⁶.

Une innovation du nouveau règlement européen consiste, sur ces questions, à rendre obligatoire l'approche dite « *privacy by design* », c'est-à-dire que les produits et services doivent être conçus et structurés dès l'origine de manière à être sobres en données¹⁴⁷. Cela rejoint parfaitement les théories de M. Lessig selon lesquelles l'architecture technique peut renforcer ou affaiblir la loi, l'ingénieur prêter la main au Parlement ou le rendre impuissant¹⁴⁸. On peut se demander si les produits et services déjà existants seront dispensés d'une conformité à des règles qui, par nature, doivent intervenir au stade de la conception, ou si les autorités pourront exiger qu'ils soient en partie reconstruits. Les enjeux sont importants.

64. Le consentement de la personne concernée - La collecte, comme toute opération de traitement n'est licite que si au moins une condition est remplie, parmi une liste. La première possibilité qui y figure, afin de marquer sa présence, est le recueil du consentement de l'individu¹⁴⁹. Elle peut être rapprochée de la seconde : « le traitement est nécessaire à l'exécution

144. - CNIL, Pack de conformité véhicules connectés, octobre 2017, p. 26.

145. - V.supra, n°52.

146. - V.infra, n°76.

147. - Art. 25 du règlement UE 2016/679 précité, intitulé « protection des données dès la conception et protection des données par défaut ». Sur cette question, V. not. C. Zolynski, « La *Privacy by design* appliquée aux objets connectés : vers une régulation efficiente du risque informationnel ? », *Dalloz IP/IT*, 2016, p. 404 ; M. Dary et L. Benaissa, « Privacy by design : un principe de protection séduisant, mais complexe à mettre en œuvre », *Dalloz IP/IT*, 2016, p. 476.

148. - C'est la démonstration d'ensemble de L. Lessig, *Code V2*, op. cit., résumée dans le fameux mantra « Code is law » (sur lequel V.supra, n° 20).

149. - Art. 6 a) du règlement UE 2016/679 précité : « la personne concernée a consenti au traitement de ses données à caractère personnel pour une ou plusieurs finalités spécifiques ».

d'un contrat auquel la personne concernée est partie [...] »), dans la mesure où cette convention aura fait l'objet elle-même d'un consentement portant, entre autres, sur le sort des données¹⁵⁰. Les deux fondements de licéité, toutefois, ne se confondent pas : si le responsable de traitement (par exemple un gestionnaire d'email) entend collecter des informations qui ne sont pas strictement nécessaires à l'exécution du contrat (par exemple, les centres d'intérêts du client, afin de procéder à de la publicité ciblée), il devra faire approuver cette opération distinctement et ne pourra pas faire cesser le service en cas de refus.

Les deux fondements posent tout de même une difficulté commune, qui est de donner de la substance, de l'épaisseur à ce consentement. Même les contrats papier ne sont guère lus, alors qu'ils sont physiquement présentés aux parties¹⁵¹. La facilité avec laquelle les contrats passés en ligne peuvent être acceptés, en deux clics de souris, n'est probablement pas de nature à améliorer cette situation. Il ne faut certes pas renoncer à rendre les conditions d'utilisation plus claires et plus lisibles. Par exemple, la CNIL a raison de reprocher à l'un des grands acteurs du secteur d'avoir noyé dans la masse des informations capitales sur les rapprochements opérés entre ses différentes sources de données¹⁵². Mais si la politique de confidentialité n'est pas lue, le progrès sera mince. Certes, le consentement doit être spécial, c'est-à-dire que « Si le consentement de la personne concernée est donné dans le cadre d'une déclaration écrite qui concerne également d'autres questions, la demande de consentement est présentée sous une forme qui la distingue clairement de ces autres questions [...] »¹⁵³. En pratique, toutefois, cela risque de se limiter à une simple case supplémentaire à cocher. Il faut donc considérer avec intérêt l'idée d'utiliser, en sus des politiques de confidentialité écrites, un ensemble de pictogrammes¹⁵⁴. Proposées par la fondation Mozilla, ces

150. - *Ibid.*, 6 b) : « le traitement est nécessaire à l'exécution d'un contrat auquel la personne concernée est partie ou à l'exécution de mesures précontractuelles prises à la demande de celle-ci ».

151. - V. par ex. G. Chantepie, « l'exigence de clarté dans la rédaction du contrat », *Revue des contrats*, n° 2012/3, p. 989 : « De fait, on ne lit pas ses contrats. Une étude empirique, et dépourvue de toute prétention scientifique, menée auprès d'universitaires, dont certains spécialistes du droit du contrat, d'avocats, de magistrats, de personnes dont la capacité à débusquer les clauses les plus retorses n'est pas douteuse, conduit à dresser un constat sans appel. Pas plus que les autres ils ne perdraient trente minutes au guichet de leur banque pour vérifier si les conditions générales de leur carte bancaire ne recèleraient pas quelque clause nouvelle et contestable. ».

152. - « ... la mention de cette faculté de combinaison n'apparaît qu'au milieu des règles de confidentialité [...]. [...] alors qu'elle a trait à une modification essentielle de la politique de confidentialité de la société, (elle) n'est donc pas accessible aux utilisateurs en première intention. Par ailleurs, elle ne se distingue pas des développements qui l'entourent, eux-mêmes formulés en termes généraux notamment quant à la description des traitements de données, comme il a été dit plus haut. Il est donc impossible de considérer en l'espèce que le fait de cliquer sur la case "J'accepte" des conditions d'utilisation puisse être considéré comme un accord explicite et spécifique à cette combinaison » : délibération CNIL n° 2013-420 du 3 janvier 2014 de la formation restreinte prononçant une sanction pécuniaire à l'encontre de la société Google Inc.

153. - Art. 7, 2) du règlement UE 2016/679 précité.

154. - Le Conseil National du Numérique a manifesté son intérêt pour cette démarche de la fondation Mozilla dans son rapport *Neutralité des plateformes. Réunir les conditions d'un environnement numérique ouvert et*

icônes porteraient sur la durée de conservation des données, l'utilisation par des tiers, la transmission à des régies publicitaires, la fourniture de données aux autorités même lorsque la loi applicable ne l'exige pas¹⁵⁵.

Le groupe des CNILS européennes, anciennement appelé G29, a adopté des lignes directrices exposant ce qu'il considère comme un consentement d'une qualité suffisante au regard du RGPD¹⁵⁶. La Quadrature du Net estime, entre autres reproches, que certains grands acteurs du numérique violent ces règles relatives au consentement¹⁵⁷. L'association a organisé le dépôt de plaintes collectives, qui sont en cours d'instruction par la CNIL.

Précisons encore que le consentement doit être donné par les parents lorsqu'il concerne des données relatives à des enfants d'un certain âge. Cet âge est fixé par le règlement à 16 ans maximum, mais les États pourront placer la barre — de ce qu'on pourrait appeler la « majorité informationnelle » — plus bas, jusqu'à un plancher de 13 ans, ce qui semble bien jeune¹⁵⁸.

65. Les autres fondements de licéité - Le règlement prévoit des alternatives au consentement de la personne concernée pour fonder la licéité du traitement. Parmi elles : un traitement rendu nécessaire — directement ou indirectement — par l'application de la loi ; la sauvegarde des intérêts vitaux d'une personne - on pense évidemment à des données de santé ; le traitement est nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'autorité publique du responsable de traitement ; le traitement est nécessaire « aux fins des intérêts légitimes poursuivis par le responsable du traitement ou par un tiers, à moins que ne prévalent les intérêts ou les libertés et droits fondamentaux de la personne concernée qui exigent une protection des données à caractère personnel, notamment lorsque la personne concernée est un enfant »¹⁵⁹. Ce dernier fondement est volontairement conçu comme le plus souple ; en nécessaire contrepartie, il est aussi le plus difficile à saisir. Interprété trop généreusement, il pourrait se transformer en une machine à faire sauter la nécessité du consentement en matière de traitement de données. La CNIL s'est cependant montrée très vigilante à cet égard. Ainsi, la société Google s'étant vue reprocher de ne pas toujours recueillir le consentement des internautes avant de procéder à des rapprochements de données, elle a fait valoir qu'« il relève de son intérêt légitime de pouvoir procéder à la combinaison des données de

soutenable, mai 2014, p. 40 : https://cnnumerique.fr/wp-content/uploads/2014/06/CNNum_Rapport_Neutralite_des_plateformes.pdf.

155. - http://wiki.mozilla.org/Privacy_Icons.

156. - G29, *Guidelines on consent under regulation 2016/679*, novembre 2017.

157. - La Quadrature du net, *Dépôt des plaintes collectives contre les GAFAM !*, article du 28 mai 2018 sur laquadrature.net. Sont visés Facebook, Google, Apple, Amazon et LinkedIn.

158. - En France, la loi précitée du 20 juin 2018 retient l'âge de quinze ans.

159. - Art. 6 du règlement UE 2016/679 précité.

ses utilisateurs (qu'ils soient authentifiés ou non) afin de leur garantir la meilleure qualité de service possible [...] »¹⁶⁰. La CNIL, appliquant des dispositions de la loi de 1978 comparables à l'article 6 du nouveau règlement européen, rappelle cependant qu'il faut procéder à une balance des intérêts (« ... à moins que ne prévalent les intérêts [...] de la personne concernée [...] »). Or, en l'espèce, « la société a prévu de procéder à la combinaison potentiellement illimitée de toutes les données qu'elle collecte sur chacun de ses utilisateurs, quel que soit leur statut, et alors même qu'elle n'a pas déterminé les durées de conservation qui leur seraient applicables. Cette combinaison est donc de nature à méconnaître les intérêts des utilisateurs et à porter atteinte à leur droit au respect de la vie privée »¹⁶¹. Dans une autre affaire, un commerçant en ligne conservait les données bancaires de ses clients au-delà de la transaction, sans les en informer. Il mettait en avant son intérêt légitime à faciliter les paiements ultérieurs et à augmenter, ce faisant, l'ergonomie du site et de l'expérience d'achat. La CNIL répondit que « [...] si l'intérêt légitime de la société justifie parfaitement la conservation de données commerciales habituelles (nom, adresse, numéro de téléphone, etc.) en contrepartie d'une information adéquate des personnes, la fourniture d'un service de portefeuille électronique, en revanche, doit être entourée de garanties renforcées. En l'occurrence, compte tenu de la sensibilité toute particulière que revêtent leurs données bancaires pour les personnes concernées, de seules mesures d'information sur la conservation de ces données associées à une faculté d'effacement ex post ne sauraient constituer de telles garanties »¹⁶². Ces motifs ont le double intérêt de constituer une seconde illustration de la « balance des intérêts » opérée par la CNIL pour neutraliser le caractère volatil de la notion « d'intérêt légitime » du responsable de traitement, et de rappeler que toutes les données n'ont pas la même « sensibilité ».

66. L'information de la personne — Quel que soit le fondement de licéité retenu, la personne dont les informations sont collectées doit recevoir un certain nombre d'informations. Il s'agit notamment de l'identité du responsable de traitement, des finalités du traitement, des destinataires des données, du fait que le responsable de traitement entend transférer ces données à l'extérieur de l'Union européenne¹⁶³. S'ajoutent encore, par exemple, la durée de conservation des données, ou l'existence de droits que l'individu peut prendre l'initiative d'exercer : droit d'accès, de rectification, d'effacement, d'opposition... - ils seront examinés plus loin¹⁶⁴.

160. - Délibération CNIL n° 2013-420, précitée.

161. - *Ibid.*

162. - Délibération de la formation restreinte n°2012-214 du 19 juillet 2012 portant avertissement à l'encontre de la société X.

163. - Art. 13, 1) du règlement 2016.679 précité.

164. - V.infra, n° 99 et s.

67. **Les « catégories particulières » de données** - À plusieurs reprises, nous avons mobilisé l'image d'un noyau constitué par l'identité stable de la personne, autour duquel s'enroulent, par couches, des données de moins en moins intimes à mesure qu'on progresse vers la périphérie. Depuis la loi de 78 dans sa version originelle jusqu'au règlement européen de 2016, certaines données faisant partie du noyau, ou en contact direct avec lui, connaissent un régime juridique distinct¹⁶⁵. Le principe est l'interdiction de tout traitement de données « qui révèle l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale, ainsi que le traitement des données génétiques, des données biométriques aux fins d'identifier une personne physique de manière unique, des données concernant la santé ou des données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique ». Cette interdiction est aussitôt assortie d'une série d'exceptions¹⁶⁶.

Ainsi la protection conférée à l'identité numérique n'est-elle pas uniforme : plus faible s'agissant des couches extérieures, elle se fait plus ferme lorsque s'agissant des couches de données les plus intimes. Le principe d'interdiction reçoit cependant de nombreuses exceptions, parmi lesquelles on retrouve par exemple le consentement — sauf lorsque le droit de l'Union ou les droits internes décident qu'il est inefficace en la matière — ou les données « manifestement rendues publiques par la personne concernée » - sans quoi c'en serait fini de certains réseaux sociaux, comme Facebook, qui reposent souvent sur la mise en scène, par l'individu, de sa propre intimité.

68. **Des « formalités préalables » à « la responsabilisation »** - Une fois qu'il a déterminé les caractéristiques fondamentales de sa collecte — ou, plus largement, de son traitement — de données personnelles, que doit faire le responsable ? En réaction à l'affaire SAFARI¹⁶⁷, dans laquelle l'administration avait œuvré à l'interconnexion de bases de données en toute opacité, la loi de 1978 avait mis en place un ensemble de « formalités préalables » à accomplir avant tout traitement automatisé. Le contexte explique que les personnes publiques — et les personnes privées gérant un service public — aient été particulièrement visées : leurs traitements devaient être autorisés par un acte réglementaire pris après un avis motivé favorable de la CNIL ou, à défaut, un avis conforme du Conseil d'État¹⁶⁸. Pour les personnes privées, une déclaration préalable comportant un grand nombre de mentions obligatoires était en principe suffisante¹⁶⁹. Cette formalité

165. - Art. 31 de la loi 78-17 précitée dans son premier état ; art. 8 de la loi dans sa version actuelle ; art. 9 du règlement UE 2016/679 précité.

166. - Art. 9 du règlement UE 2016/679 précité.

167. - V.supra, n°47.

168. - Art. 15 de la loi 78-17 précitée dans sa rédaction initiale.

169. - Art. 16 et 19 de la même loi.

était encore allégée pour les traitements les plus courants et les moins dangereux¹⁷⁰. La déclaration devait comporter l'engagement de se conformer à la loi — ce qui constitue une curieuse et inutile imitation du paradigme contractuel — et donnait le droit de débiter les traitements sans attendre¹⁷¹. En revanche, le fantôme de SAFARI rôdant, toute utilisation du numéro RIN, même par un responsable de traitement privé, devait être autorisée par un décret en Conseil d'État après avis de la CNIL¹⁷². Dans la rédaction actuelle de la loi de 78, à jour de la directive de 1995¹⁷³, le droit des formalités préalables a évolué, pour devenir nettement plus complexe. Relevons que les données sensibles donnent lieu non pas à simple déclaration, mais à autorisation de la CNIL, et que leur champ inclut, mais dépasse largement le NIR: on y trouve par exemple des données génétiques et de santé, des données relatives à des infractions pénales ou encore des traitements autorisés « comportant des appréciations sur les difficultés sociales des personnes »¹⁷⁴.

Le système prévu par le règlement de 2016 est tout différent. On aurait tort de croire que ce texte vise exclusivement la protection des citoyens européens. Un autre objectif est affiché, d'importance au moins égale : le développement d'un marché unique des données. La directive de 1995 ayant été transposée de manière trop diverse, le règlement est l'occasion pour l'Union de reprendre la main et d'imposer un cadre de travail homogène, qui réponde aux attentes des professionnels du secteur¹⁷⁵. Malgré les réticences des négociateurs français, le système des formalités préalables, jugé trop lourd par les professionnels, a donc été abandonné au profit d'une « approche fondée sur le risque » d'inspiration anglo-saxonne¹⁷⁶. Le principe retenu est celui de la « responsabilisation » (*accountability*, en version originale) : le professionnel procède à un diagnostic de sa propre situation, en doit en tirer de lui-même les conséquences adéquates.

« Compte tenu de la nature, de la portée, du contexte et des finalités du traitement ainsi

170. - Article 17 alinéa 2 de la même loi.

171. - Art. 16 de la même loi.

172. - Art. 18 de la même loi.

173. - Directive 95/46/CE précitée.

174. - Art. 25 de la loi 78-17 dans sa rédaction actuelle.

175. - Sur ce point V. par ex., dans le règlement UE 2016/679 précité, le considérant 9, selon lequel les différences de législation constituent « un obstacle à l'exercice des activités économiques au niveau de l'Union » et « fausser la concurrence [...] ».

176. - « Dans son évaluation du cadre juridique actuel, la Commission relevait que ces formalités se traduisent par un coût très élevé pour les entreprises, obligées de les respecter dans chacun des États membres où elles opèrent, suivant des modalités variant d'un État à l'autre. Pour promouvoir un marché intérieur des données personnelles, l'objectif de la réforme était donc de supprimer les formalités préalables. Le projet initial de règlement consacrait ainsi une approche plus anglo-saxonne de responsabilisation des acteurs reposant sur une évaluation des exigences à respecter par l'opérateur lui-même » : E. Brunet, « Règlement général sur la protection des données à caractère personnel. Genèse de la réforme et présentation globale », *Dalloz IP/IT*, 2016, p. 567. Mme Brunet a fait partie de l'équipe française de négociation.

que des risques, dont le degré de probabilité et de gravité varie, pour les droits et libertés des personnes physiques, le responsable du traitement met en œuvre des mesures techniques et organisationnelles appropriées pour s'assurer et être en mesure de démontrer que le traitement est effectué conformément au présent règlement. Ces mesures sont réexaminées et actualisées si nécessaire »¹⁷⁷.

Une telle solution serait difficilement défendable si elle n'était pas adossée à des sanctions très élevées, susceptibles d'être infligées à celui qui n'aurait pas joué le jeu de cet autocontrôle¹⁷⁸. De plus, lorsque le professionnel constate que son traitement est « susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques », il doit se livrer à une étude d'impact complète¹⁷⁹. Ce n'est que lorsque le résultat de cette étude confirmera les inquiétudes initiales qu'il devra prendre attache avec sa CNIL, qui fournira un avis et pourra, au besoin, user de ses pouvoirs de contrainte¹⁸⁰.

Toutefois, s'agissant de certains traitements particulièrement risqués, la loi française permet à la CNIL de revenir si nécessaire à une logique de formalités préalables : il en va ainsi en cas d'utilisation du NIR ou de mise en œuvre de traitement de données biométriques¹⁸¹.

Les règles relatives à la collecte de données ainsi décrites, voyons à présent dans quel cadre se déroule leur exploitation.

B - L'exploitation des données

69. La durée de vie des données - Fragments d'information semés derrière elles par les personnes physiques, les données à caractère personnel constituent une matière première à part, qui nécessite des précautions d'emploi particulières. Constatons d'abord qu'elles ne survivent pas à l'écoulement du temps.

Une première limite, contingente, tient à la durée pendant laquelle elles restent exactes. Lorsque le professionnel a connaissance que des données qu'il détient ne sont plus conformes à la réalité, elles doivent être « effacées ou rectifiées sans tarder », de sa propre initiative¹⁸². Une seconde limite,

177. - Art. 24, 1) du règlement UE 2016/679 précité.

178. - V.infra, n°77.

179. - Article 35 du règlement UE 2016/679 précité : « analyse d'impact relative à la protection des données ». Afin d'éviter que l'appréciation de ce « risque élevé » ne soit totalement subjective, le texte énumère des hypothèses dans lesquelles l'analyse est « requise », et donne aux autorités de type CNIL la possibilité d'édicter des listes comportant des hypothèses supplémentaires.

180. - Art. 36 du même règlement.

181. - Art. 1^{er} et 11 de la loi du 20 juin 2018.

182. - Art. 4, c) du même règlement. Cela, sans préjudice du droit donné à l'individu de porter à la connaissance du professionnel cette inexactitude, en exigeant la modification.

absolue, oblige le professionnel à fixer une durée de conservation, dont la personne aura été informée, après l'écoulement de laquelle les données devront nécessairement disparaître¹⁸³. Limiter la vie des données dans le temps, c'est garantir nos avatars numériques tout à la fois contre l'écrasement — des signaux et des traces, certes fidèles, s'accumuleraient toute la vie en une oppressante montagne — et contre la défiguration - des informations non mises à jour forment une image trompeuse de l'individu¹⁸⁴.

70. La sécurité des données - S'il est interdit de conserver les données pour une durée excessive, il serait tout aussi fautif de les laisser se perdre, être corrompues ou dérobées. Cela impose de les protéger à la fois contre des incidents techniques, mais aussi contre les agressions délibérées orchestrées par des tiers. La modification volontaire des données par un agresseur est ainsi une hypothèse terrible. Qu'il s'agisse d'un groupe sanguin dans les fichiers d'une clinique, du solde d'un compte courant ouvert auprès d'un établissement de crédit, ou de la qualité d'allocataire d'une prestation sociale auprès d'une administration, on mesure à quel point elle serait inacceptable. Le risque de perte semble presque aussi redoutable. Il peut résulter d'un simple accident — des serveurs contenant des données non dupliquées sont détruits par un incendie — ou d'un chantage mafieux. Cette dernière hypothèse est celle des rançongiciels » (*ransomware*), qui se multiplient depuis peu¹⁸⁵. Il s'agit de programmes malveillants qui chiffrent les données rencontrées, et proposent ensuite de révéler la clé contre remise d'une rançon. En France, des particuliers, des entreprises, mais aussi des laboratoires d'analyse ou des hôpitaux en ont déjà été victimes¹⁸⁶. Mais l'hypothèse la plus médiatisée est probablement celle dans laquelle des données précieuses sont dérobées. Il peut s'agir, pour les pirates, de les exploiter directement ou de les revendre à des tiers : ainsi des données relatives à des moyens de paiement¹⁸⁷. Il peut encore s'agir de rendre les données

183. - Art. 13, b) du même règlement : doivent être fournis à la personne « la durée de conservation des données à caractère personnel ou, lorsque ce n'est pas possible, les critères utilisés pour déterminer cette durée ».

184. - Un contre-exemple récent peut être visité, celui de la société Cdiscount, mise en demeure par la CNIL pour conservation des informations sans limite de durée, et utilisation de cookies d'une durée de 30 ans : <https://www.cnil.fr/fr/cdiscount-avertissement-et-mise-en-demeure-pour-de-nombreux-manquements>.

185. - L'ANSSI définit le rançongiciel ainsi : « Technique d'attaque courante de la cybercriminalité, le rançongiciel ou ransomware consiste en l'envoi à la victime d'un logiciel malveillant qui chiffre l'ensemble de ses données et lui demande une rançon en échange du mot de passe de déchiffrement » (<https://www.ssi.gouv.fr/administration/principales-menaces/cybercriminalite/rancongiel/>). Un tel logiciel malveillant frappe souvent directement la personne physique ou l'entreprise dont émanent les données, mais il pourrait également s'attaquer à des responsables de traitement soumis au règlement.

186. - O. Dumons, « Des hôpitaux français eux aussi victimes de chantage informatique », article lemonde.fr, rubrique pixels, du 24/02/16. Plus récemment, le ransomware Wannacrypt a causé d'importants dégâts dans plus de 150 pays. En France, des usines Renault ont par exemple été touchées : V. Hermann, « WannCrypt : une infection "jugulée", le point sur la situation », article nextinpact.com du 15 mai 2017.

187. - Sur le phénomène, V. par ex. Observatoire de la sécurité des cartes de paiement, *Rapport annuel 2015*, spéc. p. 50 et s., consultable sur observatoire.banque-france.fr.

publiques, ou de menacer de le faire. Un célèbre site de rencontres nommé Ashley Madison a fait l'objet d'intrusions suivies de chantage. Contre une forte somme d'argent, les pirates proposaient de ne pas révéler les données des 36 millions de comptes utilisateurs, comportant notamment leur orientation sexuelle et leurs infidélités conjugales. Le site n'ayant pas payé, les données ont été dévoilées¹⁸⁸. Cette affaire illustre parfaitement les liens entre protection des données à caractère personnel et protection de la vie privée. Avant l'ère numérique, pouvait-on imaginer que des individus malveillants se retrouvent en mesure, en quelques jours d'efforts, de porter des atteintes profondes et irréversibles à la vie privée, familiale, à l'honneur et à la réputation de plusieurs dizaines de millions de personnes ?

Il appartient aux responsables de traitement de prendre les mesures nécessaires pour éviter ces différentes formes de compromission des données qu'ils exploitent¹⁸⁹. Si par malheur elles se révélaient insuffisantes, le règlement européen impose, en cas de « violation de données à caractère personnel » suffisamment grave, d'en avertir l'autorité publique ainsi que la personne concernée¹⁹⁰. Il n'est en revanche pas prévu de rendre l'incident public. Nous verrons plus loin quelles sanctions les autorités de contrôle sont susceptibles de prononcer¹⁹¹.

Quant aux comportements des pirates, ils tomberont sous le coup des incriminations figurant aux articles 323-1 et suivants du Code pénal, qui concernent les « atteintes aux systèmes de traitement automatisé de données »¹⁹². Évoquer un « vol » de données est une facilité de langage, car cette infraction est mal adaptée aux choses immatérielles¹⁹³.

71. Les décisions automatisées - Les précautions ci-dessus décrites étant respectées, quels sont concrètement les usages jugés dangereux par le pouvoir normatif, et encadrés ? Dès sa version initiale, la loi « informatique et libertés » abordait la question des décisions prises par des algorithmes sur le fondement des données. Ces textes posaient qu'aucune décision de justice « ne peut avoir pour fondement » un traitement automatisé d'informations ; quant aux décisions

188. - V. par ex. « La sécurité d'Ashley Madison “inadéquate” », article lefigaro.fr du 23/08/16.

189. - Art. 5 f) du règlement UE 2016/679 précité. : les données doivent être « traitées de façon à garantir une sécurité appropriée des données à caractère personnel, y compris la protection contre le traitement non autorisé ou illicite et contre la perte, la destruction ou les dégâts d'origine accidentelle, à l'aide de mesures techniques ou organisationnelles appropriées (intégrité et confidentialité) ; »

190. - Art. 34 et 35 du règlement UE 2016/679 précité.

191. - V.infra, n°77.

192. - Ces textes punissent notamment le fait d'accéder frauduleusement à un système de traitement automatisé de données (STAD) (art. 323-1), d'en entraver ou d'en fausser le fonctionnement (art. 323-2), d'y introduire ou d'en extraire frauduleusement des données (323-3)...

193. - V. cependant les nuances apportées, à la lecture de la jurisprudence de la Cour de cassation, par M. Daurry-Fauveau, « Le “vol d'un bien numérique : vers la suppression des guillemets », in *Les biens numériques*, éd. Ceprisca, 2015, p. 137.

administratives ou privées, elles ne peuvent être prises « sur le seul fondement » d'un même traitement¹⁹⁴. Ils proclamaient le droit pour toute personne « de connaître et de contester les informations et les raisonnements utilisés dans les traitements automatisés dont les résultats lui sont opposés »¹⁹⁵. Comme l'affirmait Jean Foyer devant l'Assemblée nationale, au moment de faire adopter la loi Informatique et libertés : « [...] l'ordinateur n'a, dit-on, aucune "faculté d'étonnement" devant les erreurs de droit ou de fait, qui peuvent affecter les données. Il n'en a point davantage devant les déductions fausses imputables au programme »¹⁹⁶. Il ne faut donc pas le laisser prendre seul les décisions importantes, sur lesquelles un regard humain doit toujours se porter.

Aujourd'hui, le règlement européen formule la solution en ces termes :

*Les États membres prévoient que toute décision fondée exclusivement sur un traitement automatisé, y compris le profilage, qui produit des effets juridiques défavorables pour la personne concernée ou l'affecte de manière significative, est interdite, à moins qu'elle ne soit autorisée par le droit de l'Union ou le droit d'un État membre auquel le responsable du traitement est soumis et qui fournit des garanties appropriées pour les droits et libertés de la personne concernée, et au minimum le droit d'obtenir une intervention humaine de la part du responsable du traitement*¹⁹⁷.

S'agissant de l'interdiction des décisions de justice fondées sur des traitements automatisés de données, l'encadrement semble plus nécessaire que jamais à l'heure des *legal tech*, ces entreprises innovantes qui tentent d'employer les méthodes du big data et de l'analyse algorithmique dans le domaine du droit. Elles ont été présentées en introduction de cette étude¹⁹⁸. Ces techniques visant à simuler ce que serait la décision de justice dans une affaire donnée vont commencer par se répandre dans les cabinets d'avocats, pour évaluer les chances de succès d'une argumentation, simuler le montant qui pourrait être obtenu pour une indemnité, arbitrer entre contentieux et transaction amiable... La tentation existera, tôt ou tard, de faire passer les algorithmes de l'autre côté de la barre

194. - Art. 2 et 3 de la loi 78-17 dans sa rédaction initiale ; art. 10 dans sa rédaction actuelle. Le texte semble bien distinguer entre les décisions de justice, qui ne pourraient utiliser des traitements automatisés, **même parmi d'autres fondements**, tandis que les décisions administratives ou privées seraient seulement tenues de ne pas se fonder **uniquement** sur un tel traitement. Ce n'est pourtant pas la solution retenue par le Conseil d'État : « si ces dispositions font obstacle à ce qu'une juridiction fonde sa décision sur les seuls résultats d'un traitement automatisé d'informations, elles n'ont en revanche ni pour objet ni pour effet de lui interdire de prendre en compte, parmi d'autres éléments d'appréciation, les résultats d'un tel traitement » (CE, 4 févr. 2004, n° 240023).

195. - Articles 2 et 3 de la loi 78-17 dans sa rédaction initiale.

196. - Compte-rendu intégral de la séance de l'Assemblée nationale du mardi 4 octobre 1977, JO, p. 5782.

197. - Art. 11, 1) du règlement UE 2016/679 précité. Adde l'art. 22, selon lequel « La personne concernée a le droit de ne pas faire l'objet d'une décision fondée exclusivement sur un traitement automatisé, y compris le profilage, produisant des effets juridiques la concernant ou l'affectant de manière significative de façon similaire », mais qui prévoit ensuite certaines exceptions.

198. - V.supra, n°16.

afin de « préparer » les décisions de justice, dans un contexte où certains magistrats croulent sous les dossiers. Cette tendance présente un grand danger.

Laissons de côté le cas particulier des décisions de justice, pour envisager plus largement la prise de décision publique sur le fondement d'un traitement algorithmique. La loi décide à présent que les destinataires de telles décisions doivent être informés de leur caractère automatisé par une mention explicite¹⁹⁹. Un texte réglementaire précise que :

L'administration communique à la personne faisant l'objet d'une décision individuelle prise sur le fondement d'un traitement algorithmique, à la demande de celle-ci, sous une forme intelligible et sous réserve de ne pas porter atteinte à des secrets protégés par la loi, les informations suivantes :

« 1° Le degré et le mode de contribution du traitement algorithmique à la prise de décision ;

« 2° Les données traitées et leurs sources ;

« 3° Les paramètres de traitement et, le cas échéant, leur pondération, appliqués à la situation de l'intéressé ;

« 4° Les opérations effectuées par le traitement ; »²⁰⁰.

Ces droits à l'information conférés aux administrés s'ajoutent aux dispositions de droit commun relatives à l'interdiction des décisions entièrement automatisées, mais ne s'y substituent pas. La CNIL l'a rappelé au Gouvernement dans une mise en demeure très médiatisée relative à l'algorithme « admission post-bac », qui répartit les nouveaux bacheliers au sein des filières de l'enseignement supérieur. Les résultats de l'automatisme, lorsqu'ils étaient contestés, ne faisaient l'objet d'aucune véritable révision humaine, en violation flagrante de la loi informatique et libertés²⁰¹.

199. - Art. L. 311-3-1 du Code des relations entre le public et l'administration (CRPA) : « [...] une décision individuelle prise sur le fondement d'un traitement algorithmique comporte une mention explicite en informant l'intéressé. Les règles définissant ce traitement ainsi que les principales caractéristiques de sa mise en œuvre sont communiquées par l'administration à l'intéressé s'il en fait la demande ». Le texte est issu de la loi précitée n° 2016-1321.

200. - Art. R. 311-3-1-2 du CRPA, issu du décret n° 2017-330 du 14 mars 2017 relatif aux droits des personnes faisant l'objet de décisions individuelles prises sur le fondement d'un traitement algorithmique. Ce texte a été pris après une délibération de la CNIL, n° 2017-023, du 16 février 2017.

201. - Décision n° MED-2017-053 du 30 août 2017 mettant en demeure le ministère de l'Enseignement Supérieur, de la Recherche et de l'Innovation. On peut notamment y lire : « Un étudiant dont la candidature n'est pas retenue pour une formation non sélective de son choix, du fait de la position qui lui a été attribuée par l'algorithme dans le classement, ne pourra intégrer celle-ci par un autre moyen. Il en résulte qu'**une décision produisant des effets juridiques à l'égard des candidats est prise sur le seul fondement du traitement APB** dès lors que celui-ci détermine les formations post-baccalauréat auxquelles ils peuvent s'inscrire. En outre, la délégation a constaté qu'en cas de contestation de l'affectation proposée, le ministère de l'Éducation Nationale s'est limité à expliquer aux candidats que le nombre de demandes d'inscription dans l'établissement demandé excède la capacité d'accueil de celui-ci et qu'en application des critères définis à l'article L. 612-3 du code de

Dans le secteur privé, la crainte que des décisions sources d'effets juridiques ne soient prises de manière automatisée renvoie principalement aux techniques de *scoring*. Il s'agit d'attribuer une note à un dossier client, par exemple un candidat à l'emprunt bancaire, en convertissant chaque élément de son dossier en un certain nombre de points positifs ou négatifs. Une délibération de la CNIL vise à encadrer cette pratique. Elle énumère limitativement les catégories de données susceptibles d'être recueillies, en précisant qu'elles sont « choisies et pondérées en fonction du lien de corrélation qu'elles présentent avec le risque attaché à l'opération »²⁰². Cela évitera certaines pratiques professionnelles observées aux USA, qui visent à utiliser le profil du client sur un réseau social comme Facebook pour en déduire son mode de vie et, de là, le risque qu'il présente²⁰³. Surtout, la CNIL rappelle que la réglementation interdit que décision soit prise exclusivement sur la base du score : le risque est grand qu'un tel système aboutisse à une décision mécanique, selon que la note du dossier considéré est inférieure ou supérieure à une note de référence fixée par les services centraux de la banque. « En conséquence, le demandeur est systématiquement informé, en cas de rejet de son dossier de crédit par l'outil de score, qu'il peut en demander une nouvelle étude, approfondie, par un agent spécialement habilité à cette fin, à l'issue d'une phase contradictoire au cours de laquelle il aura été mis en mesure de présenter ses observations sur les principales difficultés identifiées dans son dossier [...] »²⁰⁴.

La pratique du *scoring* n'a pas vocation à se cantonner à la phase de conclusion du contrat : l'exemple des « assurances comportementales » le démontre. Lancé notamment en Allemagne par l'assureur Generali, ce contrat couvrant des risques d'invalidité ou de décès se nourrit de données de santé régulièrement transmises par l'assuré lui-même, notamment au travers d'objets connectés : une balance démontrant qu'il surveille sa ligne, un tensiomètre, une montre de fitness qui prouve qu'il court à intervalles réguliers... L'assureur n'a pas accès lui-même aux données, mais s'adosse à un « tiers indépendant » (en réalité, une filiale), qui les collecte et en tire un score : seul ce score parvient à l'assureur, qui en tire les conséquences en modulant la prime à la hausse ou à la baisse²⁰⁵.

l'éducation, le vœu d'inscription n'a pas pu être satisfait. Il apparaît, par conséquent, qu'aucun réexamen de la décision finale prise sur le seul fondement du traitement APB n'est effectué au vu des éléments fournis par les candidats souhaitant contester les décisions prises à leur égard » (souligné par nous).

202. - Délibération n° 2006-019 du 2 février 2006 portant autorisation unique de certains traitements de données à caractère personnel mis en œuvre par les établissements de crédit pour aider à l'évaluation et à la sélection des risques en matière d'octroi de crédit (décision d'autorisation unique n° AU-005). Elle a été modifiée par la délibération n° 2008-198, suite à la loi n° 2008-496 du 27 mai 2008 relative à la lutte contre les discriminations : il n'est plus possible de tenir compte du sexe du demandeur. Sur ces questions, V. par ex. C. Torres, « Le *credit scoring* : une pratique très encadrée par la CNIL », *Gaz. Pal.*, 24/07/10, n° 205.

203. - A. Williams, « How Facebook can affect your credit score », article *ft.com* du 25/08/16.

204. - *Ibid.*

205. - C. Bourdoiseau, « Generali veut réinventer l'assurance avec "Vitality" », article *argusdelassurance.com*

72. La fourniture de données comme contrepartie contractuelle - Ce qui frappe, dans ce dernier exemple, n'est pas la prise automatisée de décision. Quand bien même les données issues des objets connectés seraient analysées uniquement par des opérateurs humains, et la note fixée par eux, l'inquiétude suscitée ne faiblirait pas. Ce qui inquiète, c'est la banalisation de la fourniture de données même extrêmement intimes — quoi de plus intime que les signaux vitaux du corps ? — dans les rapports avec un professionnel. Tolérer une surveillance constante contre une baisse de prime revient en quelque sorte à battre monnaie de sa vie privée. Le modèle économique, largement répandu sur Internet, « gratuité contre données » (cédées à des régies publicitaires) relève de la même idée, poussée à son paroxysme. Nous y reviendrons en étudiant la notion de contrat à l'ère numérique.

C - La circulation des données

73. Circulation interne - Même lorsque les données restent à l'intérieur de l'Union européenne, il faut s'assurer des conditions de transfert. Rien n'est plus facile que de dupliquer des fichiers numériques et de les semer à tout vent. Aussi le règlement encadre-t-il rigoureusement le recours à la sous-traitance. Il est notamment exigé du responsable de traitement qu'il choisisse exclusivement des partenaires « qui présentent des garanties suffisantes quant à la mise en œuvre de mesures techniques et organisationnelles appropriées »²⁰⁶. Autrement dit, s'il était apparent que le sous-traitant n'avait pas la capacité ou la volonté de se conformer lui-même au règlement, le responsable de traitement peut être personnellement sanctionné. De surcroît, la chaîne de sous-traitance ne peut pas s'allonger, de nouveaux acteurs ne peuvent y prendre place sans que le responsable de traitement y ait consenti par écrit²⁰⁷.

74. Le vaste champ d'application territorial du règlement - Lors de l'adoption de la première loi informatique et libertés, la question du déplacement des données hors des frontières ne se posait pas, et il était donc logique de ne trouver dans le texte aucune disposition relative à son rayonnement au-delà du territoire français. Aujourd'hui, la situation est bien différente. L'information parcourt le monde d'un bout à l'autre en quelques millisecondes. Il ne servirait à rien de prévoir une réglementation européenne très protectrice des individus, s'il suffisait de déplacer les informations pour y échapper²⁰⁸.

du 24/06/16.

206. - Art. 28, 1) du règlement UE 2016/679 précité.

207. - Art. 28, 2) du règlement précité, qui précise toutefois que cette autorisation peut être « spécifique ou générale ».

208. - En réalité, on déplace moins les informations elles-mêmes que les serveurs sur lesquels elles sont stockées ou traitées.

Sous l'empire de la directive de 1995, le droit européen des données à caractère personnel s'applique non seulement aux responsables de traitement établis sur le territoire de l'Union, mais aussi lorsque « le responsable du traitement n'est pas établi sur le territoire de la Communauté et recourt, à des fins de traitement de données à caractère personnel, à des moyens, automatisés ou non, situés sur le territoire dudit État membre »²⁰⁹. Or, la CNIL a par exemple considéré que le seul fait de placer des *cookies* dans les navigateurs d'internautes européens revenait à employer des moyens de traitement situés en Europe²¹⁰. Ainsi, le rayonnement du texte était déjà considérable. Le nouveau règlement va plus loin encore, et ajoute les critères suivants :

Le présent règlement s'applique au traitement des données à caractère personnel relatives à des personnes concernées qui se trouvent sur le territoire de l'Union par un responsable du traitement ou un sous-traitant qui n'est pas établi dans l'Union, lorsque les activités de traitement sont liées:

a) à l'offre de biens ou de services à ces personnes concernées dans l'Union, qu'un paiement soit exigé ou non desdites personnes; ou

*b) au suivi du comportement de ces personnes, dans la mesure où il s'agit d'un comportement qui a lieu au sein de l'Union*²¹¹.

Dès lors que des produits ou services peuvent être considérés comme s'adressant à des citoyens de l'Union, le règlement s'appliquera²¹². Dès lors que l'internaute fera l'objet d'un suivi, même non nominatif, le règlement s'appliquera²¹³. L'ensemble des situations saisies est extrêmement vaste²¹⁴.

75. La limitation des transferts de données hors UE - Le second pilier de la protection des données des citoyens européens, du point de vue territorial, consiste à encadrer strictement les flux sortants d'informations. Les données quittant le territoire de l'Union tombent sous la maîtrise juridique et technique d'autres nations : cela ne peut se tolérer sans garanties suffisantes. Le

209. - Art. 4, 1, c) de la directive précitée 95/46/CE.

210. - « Il est certain qu'un fichier texte ne constitue pas, en lui-même, un traitement. Cependant, la formation restreinte relève que tant la lecture que l'écriture d'informations sur la navigateur installé sur le terminal de l'utilisateur s'effectuent par l'intermédiaire de cookies, dans le but de collecter des informations dont la société sera l'unique destinataire [...]. Par conséquent, l'ensemble des équipements et logiciels participant à ces actions d'écriture ou de lecture — y compris les cookies et les outils similaires — doivent être considérées comme des moyens de traitement » (délibération n° 2013-420 de la formation restreinte de la CNIL, précitée).

211. - Art. 3, 2) du règlement 2016/679 précité.

212. - Cela peut résulter notamment de « (...) l'utilisation d'une langue ou d'une monnaie d'usage courant dans un ou plusieurs États membres, avec la possibilité de commander des biens et des services dans cette autre langue ou la mention de clients ou d'utilisateurs qui se trouvent dans l'Union » (considérant 23 du règlement précité).

213. - Cela peut résulter notamment de « [...] l'utilisation ultérieure éventuelle de techniques de traitement des données à caractère personnel qui consistent en un profilage d'une personne physique, afin notamment de prendre des décisions la concernant ou d'analyser ou de prédire ses préférences, ses comportements et ses dispositions d'esprit » (considérant 24 du règlement précité).

214. - V. not. l'analyse de R. Perray, « La délimitation territoriale du RGPD : le champ d'application et les transferts de données hors de l'Union européenne », *Dalloz IP/IT*, 2016, p. 581.

nouveau règlement se préoccupe de surcroît des « transferts ultérieurs » : le responsable de traitement devra veiller à appliquer les règles européennes même lorsque les données exportées reprennent leur circulation quelque temps plus tard. À aucun moment on ne pourra considérer qu'elles ont fini par échapper à l'orbe du droit européen²¹⁵. Ce raisonnement peut se justifier au regard du lien entretenu par les données personnelles avec les individus dont elles émanent. Ce sont des fragments informationnels de citoyens européens que l'on transporte à travers le monde, aussi longtemps du moins que les données peuvent être qualifiées de personnelles. Ceci posé, plusieurs fondements peuvent être invoqués par un responsable de traitement qui souhaiterait exfiltrer des données hors des frontières de l'Union.

Premièrement, un tel transfert de données peut se fonder sur une « décision d'adéquation ». Une telle décision est prise par la Commission, lorsqu'elle a constaté « [...] que le pays tiers, un territoire ou un plusieurs secteurs déterminés dans ce pays tiers, ou l'organisation internationale en question assure un niveau de protection adéquat »²¹⁶. Au premier abord, la solution semble la plus simple pour une entreprise. Elle n'a qu'à vérifier que le pays visé figure sur la liste blanche constituée des pays bénéficiant d'une décision d'adéquation. Si la réponse est positive, elle n'a aucune formalité supplémentaire à accomplir. Le problème est que la Commission est faillible, et que ses décisions peuvent être contestées devant la Cour de justice de l'Union européenne. C'est ce qu'a fait M. Schrems. Utilisateur de Facebook, il savait que des données le concernant étaient envoyées par la filiale irlandaise de cette société vers les États-Unis d'Amérique. Or, à la lumière des révélations d'Edward Snowden sur le programme PRISM, il a considéré que ce pays n'offrait pas un niveau de protection adéquat²¹⁷. Cela revenait à contester la décision d'adéquation rendue par la Commission européenne dans le cadre de la « sphère de sécurité » (*Safe Harbor*)²¹⁸. L'autorité irlandaise de protection des données refusa de déjuger la Commission, mais la Cour de justice de l'Union européenne adopta une position toute différente. Examinant le droit antiterroriste américain, elle releva notamment que « [...] une réglementation permettant aux autorités publiques d'accéder de manière généralisée au contenu de communications électroniques doit être considérée comme portant atteinte au contenu essentiel du droit fondamental au respect de la vie privée »²¹⁹. Elle ajouta

215. - Art. 44 du règlement 2016/679 précité.

216. - Art. 45, 1) du même règlement.

217. - Sur ces révélations, V. par ex. la synthèse de M. Szadowski et D. Leloup, « Prism, Snowden, surveillance : 7 questions pour tout comprendre », article *lemonde.fr* du 08/08/13.

218. - Il s'agissait de 2000/520/CE: Décision de la Commission du 26 juillet 2000 conformément à la directive 95/46/CE du Parlement européen et du Conseil relative à la pertinence de la protection assurée par les principes de la « sphère de sécurité » et par les questions souvent posées y afférentes, publiés par le ministère du commerce des États-Unis d'Amérique.

219. - CJUE, 6 octobre 2015, *Maximilian Schrems c./ Data protection commissioner*, C-362/14, § 94.

qu' « [...] une réglementation ne prévoyant aucune possibilité pour le justiciable d'exercer des voies de droit afin d'avoir accès à des données à caractère personnel le concernant, ou d'obtenir la rectification ou la suppression de telles données, ne respecte pas le contenu essentiel du droit fondamental à une protection juridictionnelle effective »²²⁰. La décision d'adéquation fut invalidée, provoquant un vent de panique chez les nombreuses sociétés exportant des données européennes vers les USA. Le règlement de 2016 laisse apparaître les stigmates de l'affaire Schrems lorsqu'il commande à la Commission, s'agissant de ses futures décisions d'adéquation, d'examiner une liste de critères, parmi lesquels : « l'état de droit, le respect des droits de l'homme et des libertés fondamentales, la législation pertinente, tant générale que sectorielle, y compris en ce qui concerne la sécurité publique, la défense, la sécurité nationale [...] »²²¹. Quant au *Safe Harbor*, il a été remplacé par un nouveau mécanisme dit *Privacy Shield*. À son propos, il convient de formuler deux remarques. La première, c'est que les professionnels des données resteront quoiqu'il arrive méfiants à son égard, car rien n'interdit à la CJUE de déjuger une nouvelle fois la Commission, dans un arrêt *Schrems bis*, les progrès accomplis pouvant ne pas être considérés comme suffisants²²². la seconde, c'est que le nouveau président américain Donald Trump a peut-être fait exploser le *Privacy Shield* en signant un *executive order* écartant les citoyens non américains du bénéfice de la loi *Privacy Act*²²³. Les données à partir desquelles la Commission a prononcé l'adéquation du *Privacy Shield* sont ainsi complètement bouleversées. Les entreprises se tourneront donc avec intérêt vers les autres mécanismes permettant d'assurer un transfert de données vers un pays hors Union européenne.

Deuxièmement, donc, le responsable de traitement peut se passer de décision d'adéquation s'il justifie de « garanties appropriées »²²⁴. Cela renvoie notamment à deux mécanismes : l'utilisation, dans les contrats emportant transferts de données hors Union, de clauses type adoptées par la Commission européenne²²⁵ ; les « règles d'entreprise contraignantes » (*binding corporate rules* ou *BCR*) rédigées par l'entreprise elle-même, et soumises à l'autorité de contrôle²²⁶. Il est à craindre

220. - *Ibid.*, § 95.

221. - Art. 45, 2, a).

222. - Les CNILs européennes, regroupées au sein du « G29 » (en référence à l'article 29 de la directive précitée 95/46/CE), avaient fait part de leurs inquiétudes en ce sens dans une déclaration commune du 29/07/16 : <https://www.cnil.fr/fr/declaration-du-g29-relative-la-decision-de-la-commission-europeenne-concernant-le-privacy-shield>.

223. - *Executive order* du 25/01/17 « *Sec. 14. Privacy Act. Agencies shall, to the extent consistent with applicable law, ensure that their privacy policies exclude persons who are not United States citizens or lawful permanent residents from the protections of the Privacy Act regarding personally identifiable information* ».

224. - Art. 46 du règlement 2016/679 précité.

225. - Art. 46, c) du même règlement. Ces modèles sont consultables sur www.cnil.fr/fr/les-clauses-contractuelles-types-de-la-commission-europeenne.

226. - Art. 47 du même règlement.

que la rédaction de BCR soit trop complexe et trop coûteuse pour les entreprises de tailles petite et moyenne, et qu'elles se contentent de copier-coller les clauses types de la Commission européenne dans leurs contrats sans véritablement s'interroger sur le sens profond de ces stipulations, et sur l'inflexion des pratiques qu'elles supposent.

D - Autorités de contrôle et sanctions

76. La CNIL aujourd'hui - Lorsque la Commission nationale de l'informatique et des libertés française est instituée par la loi de 1978, l'expression « autorité administrative indépendante » semble être employée pour la première fois²²⁷. Si le mot ne lui préexistait pas, la chose en revanche était déjà connue, sous la forme de la Commission des opérations de bourse ou de la Commission de la concurrence²²⁸. La CNIL est indépendante du pouvoir politique, dispose d'un pouvoir réglementaire et d'un budget propre de 16 millions d'euros²²⁹. Ses missions sont nombreuses et étendues²³⁰. Le cœur était constitué par les « formalités préalables », dont il a déjà été indiqué qu'elles diminueront fortement lors de l'entrée en vigueur du règlement de 2016, et qui consistaient à recevoir des déclarations et à délivrer des autorisations préalables aux traitements de données²³¹. Elle peut procéder à des contrôles et prononcer des sanctions. Mais son rôle pédagogique ne doit pas être sous-estimé : la CNIL informe les professionnels et le grand public, réalise des études de terrain et de prospective, décerne des labels à des produits ou techniques respectueux du droit des données à caractère personnel.

77. La CNIL demain - Le règlement européen de 2016 crée un statut uniforme qui s'appliquera à toutes les autorités de protection des données de l'Union européenne.²³² Cela leur permettra notamment de coopérer lorsqu'un dossier concernera plusieurs États membres — ce sera fréquent — en désignant une autorité chef de file, qui coordonnera leur action et servira d'interlocuteur unique à l'extérieur.

À l'occasion de cette uniformisation, le rôle de la CNIL française évolue, et ses pouvoirs augmentent. Son rôle évolue puisqu'avec l'introduction de la nouvelle logique de « responsabilisation » des acteurs, les responsables de traitement ne prendront l'initiative d'un

227. - Art. 8 de la loi 78-17 précitée dans sa rédaction d'origine : « La commission nationale de l'informatique et des libertés est une autorité administrative indépendante ».

228. - La Commission des opérations de bourse a été créée par une ordonnance 67-833 du 28 septembre 1967 ; la Commission de la concurrence par une loi 77-806 du 19 juillet 1977.

229. - <https://www.cnil.fr/fr/le-fonctionnement>.

230. - Art. 11 de la loi 78-17 précitée, dans sa rédaction actuelle.

231. - . V.supra, n°68.

232. - Chapitre VI du règlement 2016/679 précité (articles 51 et suivants).

contact avec elle que si l'auto-diagnostic qu'ils ont réalisé révèle des dangers particuliers²³³. Par conséquent, une grande partie du terrain va devenir silencieuse. Sans les déclarations et autorisations préalables, les traitements de données ne viendront plus à la CNIL : la CNIL devra venir à eux. Son emprise sur les acteurs ne risque-t-elle pas de faiblir ? Pour l'éviter, le législateur européen accompagne la logique de « responsabilisation » d'une augmentation spectaculaire des sanctions, qui pourront aller jusqu'à 20 millions d'euros ou 4% du chiffre d'affaires annuel mondial total de l'exercice précédent²³⁴. Les grands acteurs, qui ont la certitude que leurs activités seront contrôlées, prendront certainement une telle menace très au sérieux. En ira-t-il de même des acteurs de taille plus modeste ? Le risque existe qu'ils parient sur une insuffisance des moyens de la CNIL. Le budget de 16 millions d'euros, et surtout les 192 agents de la Commission ne semblent pas suffisants pour assurer sa puissance, alors que cette institution constitue le principal rempart contre les risques très graves qui pèsent sur la vie privée et l'identité numérique des citoyens.

78. Actions de groupe - Aussi pouvait-on apprécier la modification apportée à la loi informatique et libertés par la loi de novembre 2016 dite « justice du 21^{ème} siècle ». Elle permettait en effet aux individus de se regrouper pour assurer une défense plus efficace de leurs droits en matière de données personnelles devant les juridictions.

*Lorsque plusieurs personnes physiques placées dans une situation similaire subissent un dommage ayant pour cause commune un manquement de même nature aux dispositions de la présente loi par un responsable de traitement de données à caractère personnel ou un sous-traitant, une action de groupe peut être exercée devant la juridiction civile ou la juridiction administrative compétente*²³⁵.

Toutefois ce texte était décevant, notamment en ce qu'il restreignait l'objet de l'action à la cessation du manquement, à l'exclusion de toute demande en dommages-intérêts. Pourquoi prévoir une telle possibilité d'action, et lui retirer aussitôt tout intérêt, toute efficacité et tout caractère

233. - V.supra, n°68.

234. - art. 83, 5° du règlement 2016/679 précité.

235. - Art. 43 ter, II de la loi 78-17 précitée, issu de l'art. 91 de la loi n° 2016-1547 du 18 novembre 2016 de modernisation de la justice du XXI^e siècle.

dissuasif²³⁶ ? Mais la loi de mai 2018 a fait évoluer la question, qui étend l'action de groupe aux actions en responsabilité destinées à obtenir la réparation des préjudices matériels et moraux²³⁷.

Ces actions de groupe peuvent porter aussi bien sur la violation, par le responsable de traitement, du statut impératif qui vient d'être décrit, que sur les droits octroyés aux individus afin qu'ils modèlent, s'ils le souhaitent, leur identité numérique. Ce sont ces derniers droits qu'il nous faut aborder à présent.

II - La gestion personnalisée accessible aux individus

79. **La gestion de l'identité numérique** - Les règles précédemment évoquées doivent être spontanément mises en œuvre par les responsables de traitement ou leurs sous-traitants. Elles ne requièrent ni curiosité, ni vigilance, ni prise d'initiative particulière de la part des personnes dont les données émanent. Il faut à présent aborder, à l'inverse, les principaux outils juridiques, mais aussi techniques dont peuvent se saisir les individus désireux de gérer activement leur identité numérique.

Les outils juridiques : il arrive que les textes ouvrent aux personnes des droits qui ne se mettent en action que s'ils sont invoqués. Cela suppose que leurs destinataires sachent qu'ils existent, dans quel contexte il est pertinent de les invoquer, et que les modalités pratiques fixées pour leur mise en œuvre soient efficaces.

Les outils techniques : ils intéressent le juriste à un double titre. D'abord, leur existence constitue une information dont il faut tenir compte, et qui influe sur les situations à régir. Le fait que les données des utilisateurs de téléphones soient faciles ou difficiles à dérober ; que les adresses IP constituent un système fiable d'identification ou non ; que les cookies soient majoritairement acceptés ou refusés par la population : rien de cela n'est neutre pour le droit. Consciente de cette réalité, la CNIL ne se contente pas d'informer les particuliers et professionnels sur leurs droits, mais réalise un grand nombre de fiches sur des questions de technique informatique²³⁸. Ensuite, le système juridique peut sortir d'une attitude d'observation neutre, et décider d'encourager ou de décourager l'utilisation de ces outils - par exemple le chiffrement.

236. - Le CNNum défendait des options bien plus ambitieuses : « Pour que ce recours soit pleinement activable, il est néanmoins nécessaire qu'il s'accompagne de l'extension de la capacité à agir à des associations de défense de la vie privée, des organisations syndicales de salariés ou des associations formées aux seules fins d'entreprendre l'action collective. Il est impératif qu'il permette à la fois la cessation et la suspension des traitements litigieux, mais aussi la réparation des dommages immatériels et des préjudices moraux. À l'heure actuelle, seuls les dommages patrimoniaux peuvent faire l'objet d'une réparation, or les préjudices résultant d'une atteinte au droit au respect de la vie privée ne rentrent que très rarement dans cette catégorie » (*avis n° 2015-3 relatif au projet de loi pour une République numérique*, novembre 2015, consultable sur cnnumerique.fr).

237. - Art. 25 de la loi précitée du 20 juin 2018.

238. - Par ex. www.cnil.fr/fr/configurer.

Parmi ces outils techniques et juridiques de gestion de l'identité numérique, certains doivent être mis en œuvre avant la collecte de données (A), d'autres après (B).

A - En amont de la collecte de données

80. **Restreindre, interdire** - On se souvient qu'il pèse sur les responsables de traitement une obligation de récolter le minimum de données nécessaire à la réalisation des finalités qu'ils ont fixées. Mais l'on garde également en mémoire la distance qui semble séparer cet idéal réglementaire des pratiques de terrain²³⁹. L'individu peut parfois y remédier en partie, en procédant à certains arbitrages éclairés. Ceux-ci visent tantôt à limiter la collecte de données (1), tantôt à y faire obstacle (2).

1 - La collecte rationnée

81. **Le choix du partenaire contractuel** - Dans toutes les situations, fréquentes, où la collecte de données a lieu sur la base d'un consentement, et notamment à l'occasion de la conclusion ou de l'exécution d'un contrat, il est possible d'effectuer une comparaison entre les services proposés, en fonction de leur gourmandise en informations personnelles. Puisque la fourniture de données s'apparente de plus en plus à un « prix » — qui n'est pas libellé en euros mais s'exprime en fragments d'intimité mis à nu — une compétition est susceptible de s'instaurer entre les offres²⁴⁰. À titre d'exemple, l'internaute est aujourd'hui invité à choisir entre le moteur de recherche dominant, Google Search, et certains concurrents comme l'américain DuckDuckGo ou le français Qwant. Les deux derniers affirment pratiquer la publicité non ciblée, et ne pas conserver les données personnelles de leurs utilisateurs. L'arbitrage se fait alors entre une plus grande efficacité supposée du moteur dominant et la moindre gourmandise en données de ses concurrents²⁴¹. Parfois, les termes du choix sont encore plus lisibles, puisqu'il s'agit de trancher entre une solution gratuite, mais consommatrice de données personnelles, et une solution payante²⁴². La démarche de *privacy by design*, qui consiste à concevoir un produit ou un service dès l'origine de manière à ce qu'il ne puisse pas porter une atteinte profonde à l'intimité de l'utilisateur, est théoriquement rendue

239. - V. *supra*, n°63.

240. - Sur la fourniture de données vue comme le « prix » de la prestation, V. *déjà supra*, n°73.

241. - Outre l'avantage tenant à l'anonymat, un moteur comme Duck duck go met en avant l'absence de « bulle de personnalisation » dans laquelle l'internaute se trouverait enfermé (par ex. : D. Leloup, « DuckDuckGo, le petit moteur de recherche qui monte », article *lemonde.fr* du 20/02.02). Sur cette notion de bulle informationnelle, V. *infra*, n° 171 s.

242. - Parmi de multiples exemples, on peut citer la solution de stockage de données dans le cloud SpiderOak, conseillée par Edward Snowden, chiffrée, alors qu'il existe de nombreux cloud gratuits offrant de moindres garanties de confidentialité.

obligatoire par le règlement de 2016 à compter de son entrée en vigueur²⁴³. Mais il sera difficile de dépasser rapidement le vœu pieux, et de *l'imposer* à des services déjà existants, populaires, avec d'immenses bases d'utilisateurs, qui ont été pensés à l'inverse. En revanche, certains acteurs existants ou plus vraisemblablement entrants sur le marché peuvent en faire un avantage concurrentiel, susceptible d'attirer une fraction croissante de clientèle, celle qui se préoccupe de la maîtrise de son identité numérique. Ce mouvement est qualifié de « *privacy as a service* »²⁴⁴. Tout cela est néanmoins subordonné — et la réserve n'est pas mince — à la possibilité d'instaurer une véritable concurrence, alors que le secteur du numérique se caractériserait par de puissants effets d'auto-renforcement : un réseau social, par exemple, est de plus en plus attractif au fur et à mesure que sa communauté d'utilisateurs augmente, ce qui rend l'entrée sur le marché extrêmement difficile²⁴⁵.

82. Les interfaces de paramètre de la collecte - Le choix d'un prestataire ayant une politique plutôt protectrice ou plutôt agressive en matière de données personnelles ne constitue qu'une première étape. Supposons qu'un internaute ait fait le choix d'un service gratuit et performant, mais qui cherche à recueillir sur lui un maximum de données. Aujourd'hui, une entreprise comme Google propose à ses clients de prendre un grand nombre de décisions relatives à leur compte, en procédant à des arbitrages entre protection de leur intimité et pertinence du service²⁴⁶. Par exemple, l'entreprise explique qu'elle crée « une carte privée des lieux où vous vous rendez avec les appareils sur lesquels vous êtes connecté, afin notamment de fournir de meilleurs résultats de recherche sur Google Maps et d'améliorer le calcul d'itinéraires pour vos trajets domicile-travail ». Décocher cette option provoque un avertissement sur les pertes de performance qui risquent de s'ensuivre s'agissant des services de cartographie de l'entreprise. De même, il est possible de refuser que la firme de *Mountain View* stocke les instructions vocales données par l'utilisateur, mais au prix, selon elle, d'une moindre précision dans la reconnaissance vocale et d'une limitation ou d'une perte (sans plus de précisions) de fonctionnalités de recherche vocale.

243. - V.supra, n°63.

244. - V. par ex. magush.io : « *DataRespect is a framework ensuring personal data privacy presented as a service (Privacy As A Service). DataRespect allows users to recover the perfect control of their personal data while guaranteeing that it is only used by the application they choose. DataRespect enables companies to guarantee their clients the respectful use of their personal data, and compliance with local legislation* ».

245. - Cet avantage est désigné par les économistes et concurrentialistes par la formule « *winner takes all* » : V. par ex. N. Lenois et A. Jacquinn, « Référencement en ligne et abus de position dominante : quelles problématiques pour les plateformes numériques ? », *AJ contrats d'affaires — concurrence — distribution*, 2016, p. 223. Certains contestent cependant cette idée, par ex. D. S. Evans et R. Schmalensee, « *Why winner-takes-all thinking doesn't apply to the platform economy* », article *Harvard Business Review*, *hbr.org*, 04/05/16.

246. - Ces réglages sont accessibles sur myaccount.google.com/activitycontrols.

En dépit de l'aspect quelque peu dissuasif de ces alertes au moment d'effectuer les choix, il faut reconnaître que l'existence d'un tel tableau de bord est un progrès, dont l'utilisateur peut se saisir pour gérer plus finement les contours de son identité numérique.

83. Les cookies et autres traceurs - Nous avons déjà souligné l'importance du dispositif technique appelé « *cookies* » dans la collecte de données sur les internautes²⁴⁷. Or, l'individu a la possibilité de s'opposer à ce que ces fragments d'information soient déposés sur son terminal. Actuellement, la directive relative aux communications électroniques impose d'en informer spécifiquement l'internaute²⁴⁸. À titre d'exemple, un site comme Facebook affiche un « bandeau » ainsi libellé : « Nous utilisons des cookies pour personnaliser le contenu, ajuster et mesurer les publicités et offrir une expérience plus sûre. En cliquant sur le site ou en le parcourant, vous nous autorisez à collecter des informations sur et en dehors de Facebook via les cookies. Pour en savoir plus, notamment sur les moyens de contrôle disponibles, consultez la Politique d'utilisation des cookies ». L'idée de départ est saine, mais le résultat concret décevant. D'une part, ce bandeau s'affiche trop souvent : dès lors, les internautes ont appris à les fermer aussitôt sans plus en avoir conscience. D'autre part, l'exemple choisi propose simplement à l'internaute de poursuivre sa navigation en acceptant le traceur, ou bien — implicitement — de quitter le service. En visitant le site de la CNIL, on découvre ce qu'aurait pu être un modèle vertueux : le visiteur est invité à se prononcer sur une variété de traceurs pris individuellement, qu'il peut autoriser ou interdire ; même s'il les interdit tous, cela ne l'empêche pas de poursuivre sa visite, mais modifie seulement les fonctionnalités disponibles²⁴⁹.

Le projet de règlement sur les communications électroniques pourrait constituer un progrès en la matière²⁵⁰. Dans un considérant, on peut ainsi lire :

Étant donné l'usage généralisé des cookies traceurs et autres techniques de suivi, il est de plus en plus souvent demandé à l'utilisateur final de consentir au stockage de tels cookies dans son équipement terminal. En conséquence, les utilisateurs finaux sont débordés par les demandes de consentement. Le recours à des moyens techniques permettant de donner son consentement, par exemple, à l'aide de paramètres transparents et conviviaux, peut constituer une solution à ce problème. Par conséquent, le présent règlement devrait prévoir la possibilité d'exprimer un consentement en utilisant les paramètres appropriés d'un navigateur ou d'une autre application. Les

247. - V.supra, n°51.

248. - Article 5, 3) de la directive 2002/58/CE précitée telle que modifiée par la directive 2009/136/CE précitée. En droit interne, cette exigence est reprise par l'article 32-II de la loi n° 78-17 précitée dans sa rédaction actuelle.

249. - V. sur www.cnil.fr, « gestion de vos préférences sur les cookies ».

250. - Proposition de règlement du Parlement européen et du Conseil concernant le respect de la vie privée et la protection des données à caractère personnel dans les communications électroniques et abrogeant la directive 2002/58/ce (règlement «vie privée et communications électroniques»), n° 2017/0003.

*choix effectués par l'utilisateur final lorsqu'il définit les paramètres généraux de confidentialité d'un navigateur ou d'une autre application devraient être contraignants pour les tiers et leur être opposables*²⁵¹.

L'internaute installant ou démarrant pour la première fois son navigateur devrait ainsi prendre position²⁵². Les cookies déposés par le site consulté seraient traités différemment des « cookies de tiers », ces derniers, principalement utilisés par des régies publicitaires, servant généralement à traquer l'internaute tout au long de sa navigation entre différents sites. Toutefois, certains cookies tiers servent exclusivement à réaliser des mesures d'audience et sont par conséquent moins dangereux : le projet de texte les autorise donc par principe²⁵³. Il est donc probable que la majorité des internautes donnera instruction à son navigateur de refuser les cookies tiers. Les sites pourront demander une levée de ce refus à leur seul profit (*opt-in*) : la manière dont ces exceptions seront demandées et accordées, ainsi que l'effet d'un refus persistant sur les conditions de navigation, conditionnent largement l'efficacité du dispositif²⁵⁴.

En l'état actuel, ce sont des initiatives privées qui donnent aux individus les moyens les plus intéressants de s'opposer aux traceurs tiers. Des chercheurs de Stanford et Princeton ont imaginé le système *Do Not Track* (ne pas me pister) : si cette option est activée dans le navigateur, chaque envoi de données par l'internaute comprend, en en-tête, une demande visant à ne pas faire l'objet d'un suivi²⁵⁵. Les sites sont actuellement libres de respecter ou d'ignorer cette requête, mais l'*Electronic Frontier Foundation* a mis au point un outil appelé *Privacy Badger*, qui vise à analyser en temps réel les traceurs tiers invisibles rencontrés par l'internaute et à les contrecarrer²⁵⁶. Si le fait de bloquer un traceur perturbe l'expérience de navigation, l'internaute est libre de lui redonner accès à son terminal. Un tel outil redonne du pouvoir aux personnes souhaitant conserver la maîtrise de leur identité numérique, mais il est employé par une petite minorité d'initiés. Il faut espérer que le règlement sur les communications électroniques parviendra à des résultats similaires, au profit de tous.

251. - Considérant 22 du projet de règlement précité.

252. - Art. 10, 2) du projet de règlement précité.

253. - Art. 8, 1) du projet de règlement précité. L'une des faiblesses du dispositif actuel est qu'il n'effectue pas ces distinctions entre catégories de cookies. Il n'est donc pas surprenant que l'ouverture de n'importe quel site Internet fasse apparaître un bandeau avertissant contre l'usage de traceurs, puisque l'écrasante majorité des sites a recours à des mesures d'audience qui, considérées isolément, sont relativement inoffensives.

254. - Le considérant 24 du projet de règlement précité se contente d'indiquer : « Les navigateurs Web sont encouragés à proposer aux utilisateurs finaux des moyens faciles de modifier leurs paramètres de confidentialité à tout moment en cours d'utilisation et à leur permettre de prévoir des exceptions ou d'établir une liste blanche de certains sites Web ou de préciser les sites Web dont ils acceptent toujours ou n'acceptent jamais les cookies (de tiers). ».

255. - <http://donottrack.us/>.

256. - <https://www EFF.ORG/fr/privacybadger>.

Conférer aux internautes un contrôle approfondi des *cookies* ne sera toutefois pas suffisant. Pour suivre les individus en ligne, d'autres techniques ont émergé récemment, au premier rang desquelles figure l'empreinte du navigateur. Toujours selon l'*Electronic Frontier Foundation*, très vigilante sur ces questions, l'objectif est d'identifier l'internaute sans déposer aucun fichier sur son terminal, mais uniquement en combinant des fragments d'information fournis au monde par son navigateur. Il s'agit d'informations *a priori* totalement anodines, par exemple : le type de navigateur et son numéro de version ; la liste des extensions installées et leur version ; la langue choisie ; la résolution de l'écran ; le système d'exploitation et sa version ; le fuseau horaire ; les polices d'écriture disponibles sur le terminal...²⁵⁷. La plupart de ces éléments sont nécessaires à la prise en charge technique de la navigation. Par exemple, un site doit connaître la résolution de l'écran pour s'afficher correctement. Mais la combinaison de ces réglages aboutit à un profil qui, à l'échelle de centaines de milliers de personnes, se révèle rare, voire unique²⁵⁸. Les institutions européennes sont conscientes de l'existence de ces nouvelles techniques, et le projet de règlement sur les communications électroniques est censé y remédier, mais il est trop tôt pour dire si les mesures proposées suffiront à empêcher ces pratiques très silencieuses²⁵⁹.

Face aux progrès constants des outils destinés à les pister, pour protéger leur identité, mais aussi le contenu même de leurs échanges, les individus ont la possibilité d'aller plus loin. Plutôt que de simplement réduire la collecte de données, ils peuvent chercher à l'empêcher.

2. - La collecte empêchée

84. **Plan** – Il est possible d'occulter techniquement non seulement le contenu de données (a), mais aussi l'identité des parties qui les échangent (b).

257. - La description de cette technique est accompagnée d'une proposition de test sur panopticklick.eff.org.

258. - A titre d'exemple, le navigateur de l'auteur a fourni une empreinte totalement unique par rapport aux 250 000 personnes ayant déjà réalisé le test.

259. - « La collecte d'informations relatives au dispositif de l'utilisateur final aux fins de l'identification et du suivi est également possible à distance, à l'aide de techniques telles que la "capture d'empreintes numériques", souvent à l'insu de l'utilisateur final, et peut porter gravement atteinte à la vie privée de celui-ci » : projet de règlement précité n° 2017/0003, considérant 20. En réaction, l'article 8 du projet encadre non seulement « l'utilisation des capacités de traitement et de stockage des équipements terminaux » (ce qui renvoie aux cookies), mais aussi « la collecte d'informations provenant des équipements [...] y compris sur les logiciels et le matériel ».

a – Le contenu des données

85. **Le chiffrement, masque apposé sur le contenu des données**²⁶⁰ - Nous avons déjà rencontré le chiffrement, « Janus aux deux visages », dans sa fonction d'authentification : il permet de s'assurer que l'interlocuteur en ligne est bien celui qu'il prétend être²⁶¹. Sa deuxième fonction — indissociable techniquement de la première — est d'occulter un contenu aux yeux d'un tiers observateur. Il peut s'agir de protéger des données hors-ligne (par exemple, le contenu d'un disque dur) ou le contenu d'une communication. Ainsi employé, le chiffrement a mauvaise presse. M. Bernard Cazeneuve, alors ministre de l'Intérieur, a plusieurs fois présenté cette technique comme un instrument privilégié des terroristes, qui peuvent ainsi planifier leurs crimes à l'abri des écoutes pratiquées par les services de renseignement²⁶². Une tribune publiée dans le *New York Times* par plusieurs hauts magistrats européens et américains dont M. Molins, Procureur de la République de Paris, dénonçait une « obstruction à la justice »²⁶³.

S'en tenir à une telle vision serait une erreur. Comme le relève l'Observatoire des libertés et du Numérique, les journalistes, les médecins, les avocats, les lanceurs d'alertes, mais aussi les simples citoyens ont des raisons légitimes de stocker des informations et de procéder à des communications dont le contenu ne soit pas librement accessible aux curieux²⁶⁴. D'un point de vue pratique, le chiffrement consiste à transformer le paquet de données « en clair » en une suite de caractères sans signification apparente, à laquelle il faudra appliquer une « clé » de déchiffrement pour lui restituer sa physionomie initiale. S'agissant des communications, le chiffrement asymétrique, dont les concepts principaux ont déjà été présentés, est actuellement très utilisé. Il évite aux interlocuteurs d'avoir à se concerter au préalable sur une clé commune, qu'ils devraient alors se remettre en mains propres pour être certains qu'elle ne soit pas interceptée²⁶⁵. Il leur permet d'entamer immédiatement la communication, sans s'être jamais rencontrés.

260. - À la fois sur la présentation technique du chiffrement et sur les enjeux liés à son encadrement juridique, V. le colloque « chiffrement, sécurité et libertés » du 21 novembre 2016, consultable en vidéos en intégralité à l'adresse : <https://www.lececil.org/node/19426>.

261. - V. supra, n°40.

262. - V. par ex. M. Untersinger, « Terrorisme : pour contourner le chiffrement des messages, Bernard Cazeneuve en appelle à l'Europe », article *lemonde.fr* du 23/08/16.

263. - C. R. Vance, F. Molins, A. Leppard et J. Zaragoza, « When phone encryption blocks justice », article *nytimes.com* du 11/08/15.

264. - V. *Chiffrement, sécurité et libertés. Positionnement de l'Observatoire des libertés et du numérique*, janvier 2017, spéc. p. 2 : document consultable sur [lececil.org](https://www.lececil.org). Cet Observatoire est une structure privée dont sont membres Amnesty international, le Centre de Coordination pour la recherche et l'enseignement en informatique et société, la Ligue des droits de l'Homme, la Quadrature du net, le Syndicat de la magistrature et le Syndicat des avocats de France.

265. - V. supra, n°40.

Pour savoir contre qui la protection ainsi érigée est efficace, dans le cas des échanges de données, il faut cependant se demander si le chiffrement a lieu « de bout en bout » (*end to end encryption*). Prenons l'exemple des prestataires de messagerie électronique. Il est courant qu'ils chiffrent les communications « de point à point » : entre l'utilisateur A et son prestataire, le message est en clair ; entre le prestataire de A et le prestataire de B, il est chiffré et donc protégé de la curiosité des tiers ; entre le prestataire de B et l'utilisateur B lui-même, le message est à nouveau en clair²⁶⁶. L'échange est protégé d'une attaque de type « homme du milieu », c'est-à-dire d'un attaquant qui se place au milieu de la communication et la relaie tout en l'écoutant. Mais il peut être analysé par les prestataires, aux fins par exemple de proposer de la publicité ciblée à leurs clients. De plus, à partir du moment où le message existe en clair chez le prestataire, celui-ci peut être directement attaqué par des pirates, ou requis par des gouvernements de divulguer ces informations. Inversement, lorsque le chiffrement a lieu « de bout en bout », il en résulte une confidentialité maximale. Le message sort du terminal de A déjà chiffré, et parvient au terminal de B encore chiffré. Les prestataires de service, les propriétaires des réseaux de communication, par extension les gouvernements n'y ont plus accès. De nombreux outils à destination du grand public se développent, qui offrent à leurs utilisateurs un chiffrement « de bout en bout » totalement transparent pour eux, sans leur demander de se livrer à aucune forme de configuration ou de formalité préalable, les clés étant créées sans leur intervention²⁶⁷.

Quelle peut, quelle doit être l'attitude du droit en France et dans le monde à l'égard des techniques qui viennent d'être décrites ?

86. Dégrader le chiffrement, une tentation dangereuse - Cela fait plus de quarante ans que les États, poussés par leurs services judiciaires et de renseignement, sont tentés de décourager ou d'interdire les techniques de chiffrement, qui ont été considérées en France comme des armes de guerre jusqu'à la fin des années 1990²⁶⁸. Et les inquiétudes exprimées par des ministres ou magistrats semblent au premier abord parfaitement légitimes : peut-on accepter que des informations parfois cruciales pour le bon déroulement d'une enquête pénale, ou pour la sûreté de la nation, soient irrémédiablement soustraites au regard de l'État ? Une solution parfois avancée consiste à contraindre les concepteurs de techniques de chiffrement à concevoir une « clé maître » ou des « portes dérobées ». Ces solutions techniques sont différentes, mais consistent toutes en un

266. - V. Observatoire des libertés et du numérique, *op. cit.*, p. 3.

267. - Parmi les exemples les plus célèbres, citons Signal, dont le code source est public, et la conception financée par des dons : V. whispersystems.org.

268. - C. Berthet, « Chiffrement et lutte contre le terrorisme : attention à ne pas se tromper de cible », tribune publiée initialement le 22/08/16 sur lemonde.fr par un rapporteur du Conseil National du numérique et aujourd'hui consultable sur cnnumerique.fr/tribune-chiffrement/.

secret permettant à son détenteur de contourner le problème mathématique qui rend les données illisibles : il peut donc toutes les consulter à sa guise. Malheureusement, à partir du moment où cette possibilité existe, elle peut être exercée de manière totalement invisible et il est impossible de vérifier que l'État n'en fait pas usage en dehors des procédures légales. Par ailleurs, la faille peut être recherchée et trouvée par des entités hostiles disposant de moyens suffisants comme des États étrangers, des entreprises concurrentes ou des organisations criminelles²⁶⁹.

La solution consistant à « affaiblir » volontairement le chiffrement n'est pas meilleure. Elle consiste à autoriser la transformation de données lisibles en données sans signification apparente, mais en limitant la puissance des opérations mathématiques utilisées pour accomplir la transformation. De la sorte, il suffirait de disposer d'une puissance de calcul massive pour intervertir le processus sans même connaître la clé. Une telle idée suscite au moins deux objections, chacune suffisante à la disqualifier. La première, c'est que la puissance nécessaire pour renverser un processus de chiffrement faible, on l'a dit, est loin d'être le monopole des États. Ainsi, les réseaux mafieux utilisent des logiciels malveillants pour infecter des millions d'ordinateurs à travers le monde. La puissance informatique en résultant peut être mise au service d'attaques, mais aussi de calculs mathématiques²⁷⁰. La deuxième, c'est que les cibles privilégiées des services judiciaires et de renseignement, notamment les terroristes, n'utiliseront pas les versions « affaiblies » des logiciels de chiffrement. Plusieurs outils de chiffrement fort ont un code source public : la manière de les mettre en œuvre fait à présent partie du savoir commun de l'Humanité, qui ne disparaîtra pas. Criminaliser leur utilisation ne risque pas de dissuader des individus qui cherchent à tuer des dizaines d'innocents. En revanche, le citoyen ou l'entreprise ordinaires utiliseront un chiffrement facile à briser, ce qui permettra le vol de données, empêchera les objets connectés de dialoguer avec des serveurs distants en étant à l'abri d'une prise de contrôle par des pirates, neutralisera le chiffrement dans toutes ses fonctions d'authentification déjà décrites, vitales pour l'administration en ligne, la banque en ligne ou le commerce électronique²⁷¹.

87. Le contournement du chiffrement en droit positif - Faut-il pour autant renoncer à tout encadrement ? Certainement pas. La CNIL relève que le droit positif « [...] autorise notamment les

269. - En ce sens, V. not. CNIL, *Les enjeux de 2016 (3) : quelle position de la CNIL en matière de chiffrement ?*, avril 2016 ; G. Poupard, directeur de l'Agence nationale de la sécurité des systèmes d'information, « évaluation des mesures législatives relatives à la cryptographie », article liberation.fr du 24 mars 2016 ; G29, *Statement of the WP29 on encryption and their impact on the protection of individuals with regard to the processing of their personal data in the EU*, avril 2018.

270. - Sur ces « réseaux zombies » ou botnets, V. par ex. <http://www.defense.gouv.fr/content/download/354815/5085409/file/Fiche%20Cyberdefense%20-%20Botnet.pdf>.

271. - V.supra, n°40.

réquisitions numériques, l'accès aux données de connexion, les interceptions de correspondances, les enregistrements audiovisuels, la captation de données informatiques affichées à l'écran ou introduites au clavier, ou encore le recours à des experts techniques dans le cas de données chiffrées »²⁷². Les autorités peuvent en effet avoir recours à des logiciels destinés à reproduire à distance les données affichées à l'écran ou saisies au clavier par une personne faisant l'objet d'une enquête, ce qui permet d'accéder à ses données à un moment où elles ne sont plus ou pas encore chiffrées ; par ailleurs, lorsque la machine utilisée par la personne soupçonnée d'avoir commis une infraction pénale peut être physiquement appréhendée et confiée à un expert, les autorités parviennent fréquemment à contourner le chiffrement²⁷³.

En outre, plusieurs dispositions du Code pénal visent à la remise de la clé de chiffrement par les personnes en ayant connaissance. L'un d'entre eux concerne toute personne « ayant connaissance de la convention secrète de déchiffrement d'un moyen de cryptologie susceptible d'avoir été utilisé pour préparer, faciliter ou commettre un crime ou un délit, de refuser de remettre ladite convention aux autorités judiciaires ou de la mettre en œuvre, sur les réquisitions de ces autorités délivrées en application des titres II et III du livre Ier du code de procédure pénale »²⁷⁴. Selon les circonstances, les peines encourues vont de trois à cinq ans de prison et une amende allant jusqu'à 450 000 euros²⁷⁵. Un autre texte concerne spécifiquement le malfaiteur lui-même ou ses complices. Il s'applique lorsqu'un moyen de chiffrement « a été utilisé pour préparer ou commettre un crime ou un délit, ou pour en faciliter la préparation ou la commission »²⁷⁶. Il augmente de manière significative les peines encourues pour la commission « sèche » de l'infraction, mais cette augmentation n'est pas applicable à l'auteur ou complice qui a remis sa clé de déchiffrement aux autorités sur leur demande. Il est permis de s'interroger sur la conventionnalité de ce second texte, au regard du droit reconnu à toute personne accusée d'une infraction pénale de ne pas contribuer à sa propre incrimination. Ce droit résulte tant du Pacte international relatif aux droits civils et politiques que de l'article 6 de la Convention européenne des Droits de l'Homme, tel qu'interprété

272. - CNIL, « Les enjeux de 2016... », art. préc. V. l'article 706-102-1 du Code de procédure pénale. Dans le même sens : CNNum, *Rapport prédictions, chiffrement et libertés*, septembre 2017.

273. - V. l'intervention de l'expert connu sous le pseudonyme Zythom lors du colloque précité « chiffrement, sécurité et libertés » du 21 novembre 2016.

274. - Art. 434-15-2 C. pén.

275. - La peine est en principe de 3 ans de prison et 270 000 euros d'amende (premier alinéa du texte), mais elle est portée à cinq ans et 450 000 euros « Si le refus est opposé alors que la remise ou la mise en œuvre de la convention aurait permis d'éviter la commission d'un crime ou d'un délit ou d'en limiter les effets ». Observons au passage que la formule « en limiter les effets » semble quelque peu plastique au regard des exigences du principe de légalité des délits et des peines.

276. - Art. 132-79 C. pén.

par la Cour de Strasbourg²⁷⁷. Pour que la loi française soit conforme à ces conventions internationales, elle devrait au minimum s'interpréter comme visant des documents chiffrés précis, dont l'existence et le thème général sont déjà connus des enquêteurs ; la clé de chiffrement ne devrait pas pouvoir être exigée « à l'aveugle » uniquement pour prendre connaissance du contenu d'un ensemble de données codées, dans la simple éventualité où elles auraient un rapport avec l'enquête²⁷⁸.

Un requérant a fait valoir, devant le Conseil constitutionnel, que cette disposition était contraire au droit à une procédure juste et équitable garanti par l'article 16 de la Déclaration des droits de l'homme et du citoyen de 1789 et au principe de présomption d'innocence garanti par l'article 9 de cette même déclaration²⁷⁹. Il n'a pas été entendu, les Sages jugeant ce texte conforme à la Constitution considérant que :

En premier lieu, en imposant à la personne ayant connaissance d'une convention secrète de déchiffrement d'un moyen de cryptologie de remettre ladite convention aux autorités judiciaires ou de la mettre en œuvre uniquement si ce moyen de cryptologie est susceptible d'avoir été utilisé pour préparer, faciliter ou commettre un crime ou un délit et uniquement si la demande émane d'une autorité judiciaire, le législateur a poursuivi les objectifs de valeur constitutionnelle de prévention des infractions et de recherche des auteurs d'infractions, tous deux nécessaires à la sauvegarde de droits et de principes de valeur constitutionnelle.

En second lieu, aux termes de la première phrase de l'article 29 de la loi du 21 juin 2004 mentionnée ci-dessus constitue un moyen de cryptologie « tout matériel ou logiciel conçu ou modifié pour transformer des données, qu'il s'agisse d'informations ou de signaux, à l'aide de conventions secrètes ou pour réaliser l'opération inverse avec ou sans convention secrète ». Les dispositions critiquées n'imposent à la personne suspectée d'avoir commis une infraction, en utilisant un moyen de cryptologie, de délivrer ou de mettre en œuvre la convention secrète de déchiffrement que s'il est établi qu'elle en a connaissance. Elles n'ont pas pour objet d'obtenir des aveux de sa part et n'emportent ni reconnaissance ni présomption de culpabilité mais permettent seulement le déchiffrement des données cryptées. En outre, l'enquête ou l'instruction doivent avoir permis d'identifier l'existence des données traitées par le moyen de cryptologie susceptible d'avoir été utilisé pour préparer, faciliter ou commettre un crime ou un délit.

277. - Art. 14, 3) du Pacte international relatif aux droits civils et politiques du 16 décembre 1966 ; article 6 de la Convention de de sauvegarde des droits de l'Homme et des libertés fondamentales tel qu'interprété notamment par CEDH, 25 février 1993, *Funke c. France*, n° 10588/83.

278. - Ceci par analogie avec l'arrêt CEDH, *Funke c. France*, précité. Dans le cadre du droit douanier, M. Funke avait été condamné pour refus de communication de documents. La Cour affirme « que les douanes provoquèrent la condamnation de M. Funke pour obtenir certaines pièces, dont elles supposaient l'existence sans en avoir la certitude. Faute de pouvoir ou vouloir se les procurer par un autre moyen, elles tentèrent de contraindre le requérant à fournir lui-même la preuve d'infractions qu'il aurait commises. Les particularités du droit douanier (paragraphes 30-31 ci-dessus) ne sauraient justifier une telle atteinte au droit, pour tout "accusé" au sens autonome que l'article 6 (art. 6) attribue à ce terme, de se taire et de ne point contribuer à sa propre incrimination. Partant, il y a eu violation de l'article 6 par. 1 (art. 6-1) ».

279. - Décision n° 2018-696 QPC.

Enfin, ces données, déjà fixées sur un support, existent indépendamment de la volonté de la personne suspectée.

Cette décision ne préjuge pas, bien évidemment, du résultat d'un recours qui serait formé devant la Cour de Strasbourg sur le fondement de la CEDH.

Ainsi, l'arsenal existant semble d'ores et déjà suffisant pour lutter contre les usages illégitimes du chiffrement, tout en protégeant les usages — de très loin les plus nombreux — légitimes, voire indispensables de ces techniques.

b – Les parties à une communication

88. Caractère sensible des « métadonnées » – Le chiffrement des données, lorsqu'il est utilisé dans le cadre de communications, masque le contenu de l'échange, mais pas l'origine des connexions des interlocuteurs – en particulier, leur adresse IP. Par diverses techniques de recoupement privées ou publiques déjà exposées²⁸⁰, connaître l'adresse IP d'un internaute permet souvent de remonter jusqu'à son identité stable. Ainsi, si le tiers observateur ignore le contenu de l'échange, il sait qui sont les participants. Cette information est à elle seule particulièrement sensible : savoir de telle personne qu'elle discute avec telle autre, ou qu'elle consulte telle liste de sites, c'est déjà pénétrer profondément son intimité. On se souvient par exemple comment les factures téléphoniques détaillées (les « fadettes ») de journalistes avaient été exploitées pour tenter d'identifier leurs sources²⁸¹. Le même problème se pose avec Internet.

Il existe cependant des solutions techniques destinées à masquer ces informations. Elles utilisent le chiffrement, mais font de surcroît emprunter un détour aux informations lancées sur le réseau, pour que les observateurs en perdent la trace. Nous en présenterons certaines parmi les plus connues.

89. Les réseaux privés virtuels - La première technique est celle du réseau privé virtuel. L'internaute va connecter sa machine à un serveur distant, en établissant entre eux un « tunnel », dont le contenu est généralement chiffré et donc non observable par un tiers. Ce serveur distant va servir d'intermédiaire pour accéder à un réseau privé, par exemple d'entreprise ou d'université, mais peut aussi être employé pour accéder à n'importe quel site externe. C'est cette dernière possibilité qui nous intéresse particulièrement. L'intérêt pour l'internaute est double. Premièrement, l'internaute ne révèle à son fournisseur d'accès qu'un minimum d'informations. Le FAI observe une liaison entre l'abonné et le serveur distant — le « tunnel » — mais n'en sait pas davantage, car il

280. - V.supra, n°56.

281. - Cass. crim., 6 déc. 2011, n° 11-83.970.

n'a pas la possibilité d'examiner quelles informations le serveur distant va recueillir à l'extérieur. Deuxièmement, l'internaute est protégé de la curiosité du site ou du service visité. Ce n'est pas son adresse IP qui est collectée, mais celle du serveur qui lui sert d'intermédiaire. Il peut ainsi préserver la confidentialité de sa connexion, mais aussi mentir sur sa localisation géographique. Les réseaux privés virtuels ont ainsi été popularisés auprès du grand public à la suite du succès du service de vidéo à la demande Netflix, qui propose un catalogue de contenus différents selon le pays d'où ses abonnés se connectent. Afficher artificiellement une adresse IP américaine permet d'accéder à des contenus non disponibles en France, ce qui constitue une violation des conditions d'utilisation du service²⁸². Occulter son adresse IP peut également servir à commettre des infractions pénales en rendant les enquêtes plus difficiles, qu'il s'agisse d'actes banals de contrefaçons de séries télévisées sur des réseaux d'échanges de fichiers, ou des crimes les plus graves. Le constat s'impose sans cesse d'une réversibilité des techniques, qui peuvent être employées à des fins parfaitement légitimes ou pour les motifs les plus vils, ce qui rend difficile l'adoption d'une position de principe par le système juridique.

90. The Onion Router (TOR) - La seconde technique en constitue un exemple plus flagrant encore. Il s'agit du projet *The Onion Router*, plus connu sous son acronyme TOR²⁸³. TOR consiste en un ensemble de logiciels libres, qui organisent le transport des informations sur Internet selon des modalités originales, afin de protéger l'anonymat de ses utilisateurs. Habituellement, les protocoles TCP/IP font transiter les données échangées sur les réseaux par un ensemble de points relais, qui peuvent être situés n'importe où et sont choisis en temps réel pour répartir la charge sur les réseaux de communication. Mais ces paquets d'information comportent en permanence l'adresse IP de l'expéditeur et celle du destinataire : chaque point du parcours est donc en mesure d'identifier les parties à la communication. Le réseau TOR, lui, crée un ensemble de points relais appelés « noeuds », qui sont choisis au hasard, mais auxquels un minimum d'informations est fourni. Chaque « noeud » connaît les coordonnées de celui qui le suit et de celui qui le précède, mais pas davantage. Un internaute français communiquant avec les États-Unis pourrait voir ses informations transiter par la Suède, l'Autriche, le Japon, l'Argentine puis les États-Unis. Chaque paire de nœuds forme un tunnel de communications usant de sa propre clé de chiffrement. La protection de l'utilisateur repose ainsi sur la superposition de plusieurs couches : de là vient le choix de l'oignon comme symbole. Précisons que le dernier maillon de la chaîne est susceptible de communiquer en clair avec le destinataire final. Par exemple, si l'internaute français cherche à consulter le site du

282. - Art. 4.6 des conditions d'utilisation du 01/01/17 : « (...) Vous vous engagez également à ne pas : contourner, retirer, modifier, désactiver, détruire ou faire échouer les protections du contenu dans le cadre du service Netflix [...] ».

283. - Torproject.org.

New York Times, le serveur du journal enverra ses informations sous forme lisible au client argentin (appelé « nœud de sortie »), comme il le ferait pour n'importe quel autre lecteur. Le « nœud de sortie » peut donc être espionné par celui qui l'héberge²⁸⁴. C'est que l'objectif de TOR n'est pas d'occulter le contenu des communications : il est bien de masquer techniquement la provenance et la destination des flux et, partant, l'identité des interlocuteurs. Cela est inutile, cependant, si ces identités sont révélées dans le contenu d'échanges en clair. Mais il est possible d'utiliser, en combinaison avec TOR, les techniques de chiffrement de bout en bout déjà décrites. L'anonymat est alors fortement protégé.

TOR présente un autre intérêt : celui de proposer d'accéder à des sites ou à des services « cachés ». Certains leur accolent l'appellation controversée de *dark web* ou *dark net*²⁸⁵. Ils ne sont pas recensés par les moteurs de recherche, et leur adresse — reconnaissable à son extension en .onion — doit donc être précisément connue en amont de la connexion.

Les fins les plus nobles cohabitent une fois encore avec la criminalité la plus noire. Les lanceurs d'alerte peuvent masquer l'origine et la destination des communications pour entrer en relation avec des journalistes. Des dissidents politiques peuvent créer des sites en .onion pour abriter des discours contestant des régimes autoritaires, en minimisant les risques d'être identifiés et châtiés : les « printemps arabes » ont fait usage de ces outils²⁸⁶. Les citoyens ordinaires peuvent y recourir pour échapper aux techniques de plus en plus sophistiquées, mises en œuvre par des acteurs privés à des fins marchandes, visant à traquer l'ensemble de leurs activités en ligne, à l'aide notamment de leur adresse IP²⁸⁷. À côté de ces usages légitimes, certains affirment que « le Darkweb, avec le temps, est devenu une véritable zone de non-droit où tout s'échange, s'achète, se montre. On peut ainsi y acquérir toutes sortes de drogues, des armes, des organes, des personnes vivantes ou mortes, même. On peut également y consulter des sites pédopornographiques, regarder des scènes de meurtres ou de viols tournées en temps réel, etc. Un monde d'horreur à la portée de tous »²⁸⁸.

284. - www.torproject.org/docs/faq.html.en#CanExitNodesEavesdrop. La construction du réseau repose en effet sur la contribution de volontaires, qui deviennent des relais. Des individus mal intentionnés ou des services de renseignement pourraient être tentés de se porter volontaires, pour espionner les communications dont ils seraient les nœuds de sortie.

285. - V. not. le dossier spécial « Le Darkweb : la face cachée d'Internet », *Dalloz IP/IT*, février 2017, p. 70 et s. La traduction officielle proposée au Journal officiel du 26 septembre 2017 est « Internet clandestin ». Certains spécialistes de sécurité informatique réfutent le concept même de *dark web*, par ex. R. Stamboliyska, *La face cachée d'Internet*, Larousse, 2017.

286. - A. Petit, « Visite guidée du Darkweb cybercriminel », *Dalloz IP/IT*, 2017, p. 86.

287. - V. supra, n°56.

288. - L. Saenko, « Le darkweb : un nouveau défi pour le droit pénal contemporain », *Dalloz IP/IT* 2017 p. 80.

91. **Outils et usages** – La tentation première, face à ces abominations, est d'envisager l'interdiction. Rien n'est simple toutefois puisqu'interdire les outils met fin aux bons comme aux mauvais usages. On ne songerait pas à interdire les chapeaux et les lunettes de soleil sous prétexte qu'ils sont parfois portés par des criminels cherchant à s'enfuir en toute discrétion. Il importe de focaliser les efforts du système juridique, dans un premier temps, sur le caractère licite ou illicite des usages. Si l'usage est réprimé par la loi, l'outil est alors un « simple » problème matériel que les enquêteurs doivent surmonter. Comme l'écrit le Premier avocat général à la Cour de cassation, « (...) exactement comme dans la configuration du Clearnet un cyberdélinquant est d'abord un délinquant, et comme tel relevant des mêmes lois pénales. De même, les règles de compétence du juge ne sont pas différentes sur le clear ou sur le dark, et ce qui fonctionne ici doit fonctionner là. Dès lors, s'agissant des problèmes de compétence du juge ou de la loi applicable, les infractions qui sont commises sur le Darknet justifient des mêmes approches et des mêmes solutions que celles visant les infractions commises sur le Clearnet »²⁸⁹. La suite est avant tout une question de moyens. Une enquête longue et minutieuse du FBI, qui compte dans ses rangs des informaticiens de très haut niveau, a mis fin aux activités de Silk Road, l'énorme réseau de vente de drogues du Darkweb²⁹⁰.

Le problème vient finalement de ce que le numérique multiplie la puissance des outils permettant le maniement des identités. Il permet de construire les identités numériques, en agglomérant informations fondamentales et données anecdotiques autour de l'identité stable, avec une efficacité qui ne cesse de croître, et qui menace le droit à la vie privée des individus. En réaction, des possibilités sont apparues d'agir, de communiquer, de passer des transactions en masquant totalement qui l'on est. L'identité numérique est une identité exacerbée, qui oscille sans cesse entre une trop grande transparence et une opacité excessive.

Les instruments permettant la gestion de l'identité numérique en amont de la collecte de données ayant été décrits, il faut à présent présenter ceux qui interviennent en aval.

B – En aval de la collecte de données

92. **Le droit à « l'autodétermination informationnelle »** - La phase de contrôle des données en amont de leur collecte était dominée par des outils techniques - auxquels le droit n'est certes pas indifférent, car il peut les encourager, les imposer, les freiner ou les interdire, régulant ainsi indirectement les comportements. Logiquement, on assiste, en aval de la collecte, à un retour en force de la régulation directe et des outils juridiques. Les données sont en possession d'entreprises

289. - Y. Charpenel, « Le Darkweb, un objet juridique parfaitement identifié. Le paradis, l'enfer ? », *Dalloz IP/IT*, p. 71.

290. - Y. Eudes, « Comment le FBI a fait tomber Silk Road », article *lemonde.fr* du 09/09/14.

qui les exploitent, et il est trop tard pour s'opposer techniquement à la maîtrise qu'elles exercent. Elles ne relâcheront leur emprise sur ces informations que si elles y sont contraintes par le droit. Or, l'article 1er alinéa 2 de la loi informatique et libertés, tel qu'il résulte de la loi « République numérique » du 7 octobre 2016, affirme : « Toute personne dispose du droit de décider et de contrôler les usages qui sont faits des données à caractère personnel la concernant, dans les conditions fixées par la présente loi ». Cette disposition avait été retirée du projet de loi, avant de réapparaître dans la version définitive²⁹¹. Elle s'inspire ouvertement d'une décision de la Cour constitutionnelle fédérale allemande du 15 décembre 1983, dans laquelle on peut lire : « la Constitution garantit en principe la capacité de l'individu à décider de la communication et de l'utilisation de ses données à caractère personnel »²⁹². Le règlement européen du 27 avril 2016 y fait également allusion dans un considérant : « Les personnes physiques devraient avoir le contrôle des données à caractère personnel les concernant ».²⁹³

Dans son rapport « numérique et droits fondamentaux », le Conseil d'État avait vanté cet *Informationnelle Selbstbestimmung* allemand, traduit en « droit à l'autodétermination informationnelle »²⁹⁴.

*[...] alors que le droit à la protection des données [reconnu par la Charte des droits fondamentaux de l'Union européenne] peut-être perçu comme un concept défensif, le droit à l'autodétermination lui donne un contenu positif. Il ne s'agit plus seulement de protéger le droit au respect de la vie privée, mais d'affirmer la primauté de la personne qui doit être en mesure d'exercer sa liberté. En ce sens, le droit à l'autodétermination répond davantage à l'aspiration croissante des individus à l'autonomie de décision*²⁹⁵.

La Haute juridiction administrative mettait toutefois en garde contre une mauvaise interprétation de ce concept, qui ne constitue pas un droit subjectif nouveau au contenu précisément déterminé.

[...] le droit à l'autodétermination informationnelle constitue l'objectif permettant d'offrir une véritable protection des données personnelles. Par son haut niveau d'exigence, le droit à l'autodétermination peut jouer un rôle d'aiguillon, tant pour les pouvoirs publics que pour les individus.[...] Il n'apparaît pas souhaitable d'ajouter le droit à l'autodétermination à la liste des droits déjà reconnus par les textes existants ou que la proposition de règlement de l'Union européenne envisage de reconnaître, tels que les droits d'information, d'accès, de rectification ou d'opposition. Le droit à

291. - N. Martial-Braz, « Les nouveaux droits des individus consacrés par la loi pour une République numérique. Quelles innovations ? Quelle articulation avec le Règlement européen ? », *Dalloz IP/IT*, 2016, p. 525.

292. - BVerfGE 65, 1. La traduction est de Y. Pouillet et A. Rouvroy, « Le droit à l'autodétermination informationnelle et la valeur du développement personnel. Une réévaluation de l'importance de la vie privée pour la démocratie. », in *État de droit et virtualité*, K. Benyekhlef & P. Trudel (dir.). Montréal : Thémis, 2009.

293. - Considérant 7 du règlement 2016/679 précité.

294. - Conseil d'Etat, *Étude annuelle 2014 : le numérique et les droits fondamentaux*, La documentation française, 2014.

295. - Rapport précité, p. 268.

*l'autodétermination se situe à un autre niveau : il donne sens à tous ces droits, qui tendent à le garantir et doivent être interprétés et mis en œuvre à la lumière de cette finalité [...]*²⁹⁶.

Le droit à l'autodétermination informationnelle n'est donc qu'un idéal vers lequel doivent tendre les pouvoirs publics²⁹⁷. Il leur enjoint de mettre à disposition des individus des instruments de contrôle de leurs informations, sans préciser comment. Aussi convient-il de répondre à deux questions intimement liées : l'une d'ordre théorique, l'autre d'ordre pratique. La première : quelle est la nature juridique du lien qu'entretient l'individu avec ses données (1) ? La seconde : quels moyens faut-il mettre à sa disposition pour faire advenir l'idéal que constitue le droit à l'autodétermination informationnelle (2) ?

1 - La nature du droit de l'individu sur ses données

93. Droit réel ou personnel ? - Certaines théories considèrent les données comme des choses (a), d'autres comme des prolongements de la personne (b).

a – Les théories réalistes

94. Une propriété ordinaire - Certains auteurs l'affirment : « Il semble logique que les individus soient propriétaires de leurs données »²⁹⁸. L'idée est au premier abord séduisante. La protection civile, mais aussi pénale de la propriété pourrait être mobilisée contre une collecte ou une exploitation non autorisée des informations personnelles²⁹⁹. Devenues des biens — presque — comme les autres, ces informations pourraient en revanche circuler très facilement en usant des grands contrats spéciaux comme le bail ou la vente. En d'autres termes, les données personnelles deviennent une matière première, pour laquelle il existe une offre susceptible de rencontrer une demande. Le projet de l'opérateur espagnol Telefonica semble s'inscrire dans la droite ligne d'une telle conception. L'internaute aurait accès à une plateforme recensant ses données personnelles et

296. - Rapport précité, p. 268 et 269.

297. - Pour une vive critique de l'autodétermination informationnelle, V. N. Ochoa, « Pour en finir avec l'idée d'un droit de propriété sur ses données personnelles : ce que cache véritablement le principe de libre disposition », *RFDA*, 2015, p. 1157.

298. - I. Beyneix, « Le traitement des données personnelles par les entreprises : big data et vie privée, état des lieux », *JCP G*, 9 nov. 2015, n° 46-47, doct. 1260. M. Lawrence Lessig défend également cette idée s'agissant du droit américain : « *As with copyright, a privacy property right would create strong incentives in those who want to use that property to secure the appropriate consent. That content could then be channeled (through legislation) through appropriate technologies. But without that consent, the user of the privacy property would be a privacy pirate. Indeed, many of the same tools that could protect copyright in this sense could also be used to protect privacy* » (*Code V2, op. cit.*, p. 228). L'auteur nuance sa position dans les pages suivantes, sans l'abandonner.

299. - Sur les tentatives d'appliquer l'infraction de vol à des données personnelles, V. *supra*, n°70.

pourrait faire de sa propriété un usage défensif — en refusant l'utilisation des informations — ou offensif - en négociant leur usage par les géants d'Internet contre service ou rémunération³⁰⁰. On estime à 1000 milliards la valeur économique des données qui seront produites chaque année en Europe à l'horizon 2020³⁰¹. Pourquoi ne pas permettre aux individus d'en retirer une juste part ? Le fantasme s'écroule rapidement lorsque l'on comprend que c'est l'accumulation de données, leur mise en forme, la capacité technique à les interroger de manière pertinente et l'aptitude à leur découvrir des débouchés qui recèle une valeur économique. Les données d'un individu isolé ne valent rien ou presque : quelques dizaines de centimes, tout au plus, en fonction notamment de variables socioprofessionnelles, de santé et de centres d'intérêt qui conditionnent la sensibilité aux publicités ciblées³⁰². Plus fondamentalement, le Conseil d'État critique la philosophie que sous-tend la conception réaliste des données personnelles : « Là où le droit de propriété prétend faire des individus des gestionnaires d'un patrimoine, le droit à l'autodétermination rappelle qu'ils doivent demeurer en mesure de décider de leur existence. L'un se situe sur le plan de l'avoir, l'autre sur celui de l'être »³⁰³. Le Conseil national du numérique, lui aussi, résume parfaitement les principales objections suscitées par le paradigme propriétaire en matière de données personnelles :

Le Conseil invite à exclure cette option : parce qu'elle renvoie à l'individu la responsabilité de gérer et protéger ses données, renforce l'individualisme et nie le rapport de force entre consommateurs et entreprises ; parce qu'elle ne pourrait que générer des revenus anecdotiques pour les usagers et susciter à l'inverse un marché de la gestion protectrice des données numériques ; parce qu'elle déboucherait à un renforcement des inégalités entre citoyens en capacité de gérer, protéger et monétiser leurs données et ceux qui, par manque de littératie, de temps, d'argent ou autre, abandonneraient ces fonctions au marché³⁰⁴.

95. Une propriété intellectuelle - Un autre élément troublant, s'agissant de la théorie ci-dessus présentée, c'est qu'elle occulte largement le lien intime qui devrait exister entre la personne et les données qu'elle exsude. Or, « vendre » une information personnelle n'est pas vendre une chaise ou une brosse à dents. En réaction à cette anomalie, il a été proposé par M. Chemla de recourir à cette branche spécifique du droit des biens que serait la propriété intellectuelle.

[...] en quoi nos données privées devraient-elles être traitées autrement qu'une œuvre

300. - « Telefonica veut permettre à ses clients d'être payés pour leurs données », article *leparisien.fr* du 06/09/16.

301. - V.-L. Bénabou et J. Rochfeld, *A qui profite le clic ?*, éd. O. Jacob, 2015.

302. - J. Rochfeld, « Contre l'hypothèse de la qualification des données personnelles comme des biens », in *Les biens numériques*, Ceprisca, 2015, p. 226. Le Financial Times propose à chacun de calculer la valeur de ses données : E. Steel, C. Locke, E. Cadman et B. Freese, « How much is your personal data worth ? », article *ft.com* du 12/06/13.

303. - Conseil d'État, *Etude annuelle 2014 : le numérique et les droits fondamentaux*, rapport préc., p. 268.

304. - CNNum, *Neutralité des plateformes...*, rapport préc., p. 37.

de l'esprit ? Ce qui définit une œuvre, ce qui lui confère la protection de la loi, c'est la condition d'originalité. Elle doit porter « l'empreinte de la personnalité » de l'auteur. Et qu'est-ce qui porte mieux l'empreinte de notre personnalité, sinon l'ensemble des données qui nous définissent en tant qu'être unique et que nous répétons de formulaires d'inscriptions en profils divers, et celles que nous produisons, via nos photos de vacances, nos blogs, nos commentaires et, finalement, nos vies ? Bien sûr, toutes nos productions en ligne ne sont pas des œuvres en tant que telles. Mais leur ensemble, leur addition sous forme de « profil » commercialisable auprès des plateformes de publicité, est indiscutablement unique, original, en grande partie produit par notre esprit. Presque une œuvre au sens du droit d'auteur [...]»³⁰⁵.

Retenir une telle analyse permettrait de mobiliser les deux composantes du droit d'auteur : le droit patrimonial et le droit moral. S'agissant du droit patrimonial, l'auteur anticipe la critique tenant à la modicité des rémunérations individuelles, et propose de mettre en place des organismes de gestion collectifs, sur le modèle d'une SACEM. La négociation aurait lieu à un niveau collectif, ce qui constitue une idée séduisante. Quant au droit moral, il emporte entre autres la faculté, pour l'auteur, de divulguer ou non « l'œuvre » et d'en « défendre l'intégrité » contre des usages déshonorants³⁰⁶. On ne peut se lancer dans l'étude du résultat qui serait produit par une transposition de ces règles à la question des données personnelles sans avoir affronté une objection de principe : le droit d'auteur est-il applicable ici ? Il semble que non³⁰⁷. L'œuvre de l'esprit est une « création », une « réalisation »³⁰⁸. Ce processus artistique est conscient et volontaire. C'est habilement que M. Chemla présente comme œuvre non pas les données personnelles considérées isolément — quelle « création » dans le fait de se connecter au site du Monde, suscitant l'enregistrement d'un cookie sur son navigateur ? - mais le profil complet qui les agrège toutes, autrement dit l'identité numérique de la personne. Toutefois, les nombreuses informations suscitées passivement, par exemple par le déplacement dans l'espace ou la navigation sur Internet, sont certes reliées à la personne, mais pas à la personnalité, ce qui change tout. Au sein des données personnelles, il en est qui méritent d'être qualifiées d'œuvres : ainsi de la correspondance abondante et sophistiquée entre deux individus. Mais cette qualification se surajoute au tout petit nombre de données ainsi élues parmi la masse, sans que ni les autres ni l'ensemble ne se transforment en création. Là ne peut résider la solution. Aussi a-t-il été proposé de rendre plus intense encore le lien entre données et personnes dont elles émanent.

305. - L. Chemla, « Nous sommes tous des ayants droit », article *liberations.fr/ecrans/* du 23/10/13.

306. - Articles L. 121-1 et s. du CPI.

307. - J. Rochfeld, « Contre l'hypothèse... », art. préc., p. 229 ; L. Maurel, « Le CNNum s'est prononcé contre l'instauration d'un droit de propriété privée sur les données personnelles », article *scinfolex.com* du 19/06/14.

308. - Le premier mot est utilisé par l'art. L. 111-1 du CPI, le deuxième par l'article L111-2 (« l'œuvre est réputée créée [...]).

b – Les théories personnalistes

96. Une émanation directe de la personne – Madame Rochfeld a mis en évidence les faiblesses des théories réalistes :

Parler de « bien », d'« appropriation » et de valeur, revient en réalité à faire trop peu de cas, quant à la texture de la donnée, de la composante d'identité et de personnalité de chacun que celle-ci renferme. La thèse occulte par ailleurs, quant aux risques engendrés par les utilisations rappelées, ceux de manipulations des comportements que les traitements peuvent engendrer ainsi que de révélations non souhaitées : on ne défend pas qu'un avoir, qu'une valeur économique, en défendant ses données personnelles ; on protège la personne, dans sa liberté d'agir et la conduite de sa vie privée, dans la maîtrise de ses composantes d'identité³⁰⁹.

Il faut donc refuser de considérer les données personnelles comme des biens. Leur dénomination même, le fait qu'elles sont les briques élémentaires composant, ensemble, l'identité numérique : tout indique qu'elles sont des prolongements de l'individu. Le droit à l'autodétermination informationnelle et ses différents attributs devraient donc rejoindre les droits dits « de la personnalité ». Ces droits constituent des instruments de « contrôle » et « permettent [...] à la personne d'exercer sa maîtrise des différents aspects de sa personnalité. Cette maîtrise [...] trouve plusieurs expressions. Elle peut s'incarner par exemple dans une réticence (par ex., refus d'une personne de révéler des informations sur sa vie privée ou de diffuser son image), une révélation (révélation sur sa vie privée, aveu public par une personne de sa culpabilité avant tout jugement de condamnation), une mise au point ou rectification (exercice du droit de réponse, exercice du droit de rectification prévu par la loi du 6 janv.1978) »³¹⁰. Mais ces droits n'ont-ils pas une nature entièrement extrapatrimoniale, qui s'opposerait à ce que des données personnelles soient cédées contre une rémunération ou un service ? Cette analyse est datée : il est aujourd'hui admis que l'individu puisse donner accès à son image, voire à une partie de sa vie privée, à titre gratuit ou onéreux. Cela a conduit plusieurs auteurs à reconnaître que les droits de la personnalité présentent deux faces, l'une patrimoniale et l'autre extrapatrimoniale³¹¹, ou l'une économique et l'autre morale³¹².

97. Un élément de l'intégrité morale - Les droits de la personnalité peuvent être classés selon qu'ils protègent l'intégrité physique (droit au respect du corps humain même après la mort,

309. - J. Rochfeld, « Contre l'hypothèse... », art. préc., p. 230.

310. - A. Lepage, « Personnalité (Droits de la) » in *Rép. civ. Dalloz*, octobre 2016, n° 22.

311. - Par ex. G. Goubeaux, *Traité de droit civil. Les personnes*, LGDJ, 1989, dir. J. Ghestin, n° 285, p. 256 et n° 315, p. 29.

312. - J. Antippas, « Propos dissidents sur les droits dits "patrimoniaux" de la personnalité », *RTD. com.*, 2012, p. 35.

nécessité du consentement pour les actes médicaux, pour la recherche biomédicale, pour le prélèvement d'organe d'une personne vivante...) ou l'intégrité morale (droit de réponse, droit moral de l'auteur, droit au respect de la vie privée, droit au respect de la présomption d'innocence...) ³¹³. M. Beignier estime que l'ensemble de ces droits subjectifs découle d'un seul et même droit-matrice, qui serait un droit général à la tranquillité et à la dignité de chacun ³¹⁴. Mais s'il fallait prendre position au sein d'une classification plus fine, il semble évident que le droit de l'individu sur ses données personnelles prendrait place au sein de ceux qui protègent l'intégrité morale. Plus précisément encore, il se situerait au carrefour du droit à l'image — en ce que l'identité en général, et l'identité numérique en particulier, constituent des représentations de l'individu, même s'il s'agit de représentations abstraites à vocation sociale ³¹⁵ — et du droit à la vie privée - dont le droit des données personnelles constitue le bastion avancé ³¹⁶.

Toutefois, le régime proposé par Madame Rochfeld s'agissant du droit à l'autodétermination informationnelle emprunte aussi aux protections du corps humain. Dressant un parallèle aussi riche qu'inattendu, elle mobilise le régime des produits sanguins, en ce qu'il entretient avec l'individu un lien immensément intime, mais susceptible de se distendre : « le sang ne peut faire l'objet que d'un don lorsqu'il est prélevé, mais les médicaments composés de produits sanguins, issus de sa transformation, peuvent quant à eux être cédés à titre onéreux entre professionnels » ³¹⁷. Or, poursuit l'auteur, le lien des données avec la personne dont elles émanent peut se relâcher jusqu'à disparaître, lorsque des processus d'anonymisation suffisants sont mis en œuvre. L'image est très habile, mais n'est-elle pas un peu trompeuse ? En effet, le statut du sang change à un moment clair, lié à une réalité physique : celui où il quitte le corps. Le moment où il devient impossible de rattacher une donnée à l'individu est quant à lui relatif et contingent : il tient à l'état de l'art actuariel, à la puissance des moyens de traitement mobilisés pour opérer les recoupements, et à l'existence de bases de données tierces qui pourront fournir un lien manquant entre deux fragments. Autrement dit, une donnée peut être anonyme pour les uns — ceux manquant de puissance de traitement, d'informations complémentaires ou de compétence technique — mais pas pour les autres ³¹⁸. Elle peut être anonyme aujourd'hui, mais ne plus l'être demain. Il semble préférable de

313. - Sur cette distinction, V. A. Lepage, « Personnalité... », art. préc., n° 25 et s.

314. - B. Beignier, *L'honneur et le droit*, LGDJ-Lextenso, 2015, p. 53 ; comp. J.-M. Bruguière et B. Gleize, *op. cit.*, n° 16, qui trouvent l'idée séduisante, mais estiment que « (...) cette unité n'est pas aujourd'hui à l'œuvre et que la théorie des droits de la personnalité reste à construire ».

315. - V. *supra*, n° 29 s.

316. - V. *supra*, n° 60.

317. - J. Rochfeld, « Contre l'hypothèse... », art. préc., p. 232.

318. - V. déjà, sur la frontière entre l'information pseudonyme et l'information anonyme comme critère de déclenchement du droit des données personnelles, *supra*, n° 58.

prendre acte de cette frontière mouvante entre le personnel et l'anonyme en rattachant exclusivement l'autodétermination informationnelle à la sphère de l'abstrait et de l'intellectuel. Cela implique qu'une donnée qui s'était détachée de l'individu peut retrouver son lien ultérieurement : l'idée est inconfortable, mais techniquement réaliste.

98. Une possible gestion collective - En revanche, nous suivrons volontiers l'auteur lorsqu'elle affirme qu'une approche personnaliste des données personnelles n'est pas incompatible avec une dimension collective. M. Chemla appelait de ses vœux une « SACEM » des données personnelles³¹⁹. Il n'est pas nécessaire de considérer les informations personnelles comme protégées par le droit d'auteur pour imaginer que les utilisateurs d'un grand service en ligne se fédèrent pour négocier des contreparties. Il s'agit de conclure des contrats — similaires à ceux qui sont passés en matière de droit à l'image — et cette conclusion s'accommode sans difficulté de représentations collectives. Comme l'écrit M. Casilli, « Je pense que les internautes vont s'unir et s'organiser pour défendre leurs intérêts en tant que fournisseurs de données. Pour cela, ils vont s'inspirer des associations de défense des consommateurs, ou même des syndicats ouvriers. Seule une réponse collective et solidaire pourra rétablir l'équilibre »³²⁰.

La nature juridique du lien unissant l'individu à ses données personnelles est à présent connue : il s'agit d'un droit de la personnalité, voisin du droit à l'image et du droit au respect de la vie privée. Quelles sont, à présent, les prérogatives juridiques précises et concrètes qui permettent à la personne d'assurer un contrôle de ces informations ?

2 - Les composantes du droit de l'individu sur ses données

99. Plan - On peut les regrouper en cinq catégories : la personne est autorisée à connaître les données (a), à les faire modifier ou supprimer dans certains cas (b), à obtenir certains déréférencements de la part de moteurs de recherche (c) à récupérer ses données (d), à les transmettre après sa mort (e).

a. – Le droit de connaître ses données

100. Le droit d'accès - Dès 1978, un certain nombre de droits ont été octroyés aux individus, qu'ils doivent prendre l'initiative d'exercer. On les retrouve dans la version contemporaine de la loi informatique et libertés, ainsi que dans le règlement européen de 2016.

319. - V.supra, n°95.

320. - A. Casilli, « Contre l'hypothèse de la "fin de la vie privée" », *Revue française des sciences de l'information et de la communication*, n° 3, 2013.

Le droit d'accès est le plus fondamental : il conditionne tous les autres. Il permet notamment à une personne de contacter un responsable de traitement pour lui demander si des données la concernant sont détenues et, en cas de réponse positive, quelle est leur consistance précise et exhaustive³²¹. D'autres informations peuvent être obtenues, en particulier les finalités du traitement. L'exercice du droit est quasi-gratuit : seul l'équivalent des frais de reproduction peut être exigé. Le responsable de traitement ne peut refuser de répondre que s'il démontre que les demandes sont « manifestement abusive »³²². Il s'agit, selon le mot de Jean Foyer, de faire des fichiers informatisés « des maisons de verre »³²³.

101. **Un droit ciblé** - Le seul obstacle sérieux à l'exercice de ce droit, c'est qu'il ne sera exercé que si la personne a des raisons de croire, *a priori*, qu'un responsable de traitement donné dispose d'informations sur elle. Certes, nous avons vu qu'elle bénéficie d'un droit d'être informée des traitements la concernant, y compris ceux qui ne reposent pas sur son consentement³²⁴. Mais la règle connaît des exceptions et, surtout, elle pourrait ne pas être respectée³²⁵. Il n'existe pas de mécanisme permettant à l'individu d'interroger la CNIL, par exemple, pour obtenir la liste des fichiers dans lequel il se trouve, ou d'avoir une quelconque vue d'ensemble des données le concernant.

Une fois l'individu assuré de la présence de données personnelles à lui rattachées dans un fichier, et après qu'il ait été informé de leur teneur, le voici en mesure d'en demander, le cas échéant, la modification ou la suppression.

b – Le droit de faire modifier ou supprimer ses données

102. **Le droit de rectification ou d'effacement**³²⁶ - Aux termes de la loi informatique et libertés, « Toute personne physique justifiant de son identité peut exiger du responsable d'un traitement que soient, selon les cas, rectifiées, complétées, mises à jour, verrouillées ou effacées les données à caractère personnel la concernant, qui sont inexactes, incomplètes, équivoques, périmées, ou dont la collecte, l'utilisation, la communication ou la conservation est interdite »³²⁷. L'identité numérique est l'un des visages que l'individu présente au monde. La fausseté, l'incomplétude et l'obsolescence

321. - Art. 39, 40 et 41 de la loi 78-17 précitée, dans sa rédaction actuelle ; art. 15 du règlement 2016/679 précité.

322. - « [...] notamment par leur nombre, leur caractère répétitif ou systématique » (art. 39 de la loi 78-17).

323. - Compte-rendu de la séance de l'Assemblée nationale du 4 octobre 1977, précité, p. 5783.

324. - Art. 13 et 14 du règlement 2016/679 précité.

325. - Sur les exceptions, V. not. l'art. 14, 5° du règlement 2016/679 précité.

326. - L'art. 40 de la loi 78-17 traite ensemble de la rectification et de l'effacement, tandis le règlement 2016/279 leur consacre deux articles distincts (16 et 17).

327. - Art. 40, I de la loi 78-17 précitée.

des informations le déforment. Le responsable de traitement qui s'en apercevrait doit agir sans attendre qu'on le lui demande³²⁸. Mais il est évident que la personne concernée est la plus apte, d'une part à déceler ces informations inexactes ou périmées, d'autre part à choisir comment y remédier : en les remplaçant par le vrai ou par le vide. Un peu à part est l'hypothèse des données dont le traitement était interdit : il faudrait comprendre pourquoi cette interdiction s'est révélée ineffective, et pourquoi la vigilance de la personne concernée s'est révélée nécessaire au respect des règles en vigueur.

103. Le droit d'opposition - Dernier membre de la trilogie des droits classiques issus de la première loi informatique et libertés, il permet à une personne « de s'opposer, pour des motifs légitimes, à ce que les données à caractère personnel la concernant fassent l'objet d'un traitement »³²⁹. Ce droit peut s'exercer en amont du traitement, mais également à tout moment par la suite. S'il s'agit de s'opposer à l'utilisation de données à des fins de prospection commerciale, il n'y a pas à fournir de motif particulier³³⁰. Dans les autres cas, la personne doit expliquer quels sont les motifs légitimes qu'elle invoque, et le responsable de traitement est en droit de les contester. Enfin, certains traitements, notamment ceux répondant à des obligations légales, échappent totalement au droit d'opposition, ce qui est logique³³¹.

c. - Le droit au déréférencement (dit « droit à l'oubli »).

104. Présentation - Le « droit à l'oubli », d'origine jurisprudentielle et d'invention beaucoup plus récente, se présente comme un prolongement des droits « de première génération » qui viennent d'être présentés. La Cour de Justice de l'Union européenne fait preuve d'audace en matière de protection des données personnelles. Avant l'arrêt *Schrems*³³², la décision *Google Spain* l'avait déjà démontré de manière éclatante³³³.

328. - V.supra, n°69.

329. - Art. 38 al. 1 de la loi 78-17 précitée.

330. - Art. 38 al. 2 de la loi 78-17 précitée.

331. - Art. 38 al. 3 de la loi 78-17 précitée.

332. - V.supra, n°75.

333. - CJUE, 13 mai 2014, *Google Spain SL, Google Inc. c./ Agencia Española de Protección de Datos (AEPD), Mario Costeja González*, C-131/12 : RLDI, août 2014, n° 107, p. 32, note O. Pignatari ; *RJPF*, juill. 2014, n° 7, p. 19, note S. Maucclair ; *JCP G*, juin 2014, n° 26, p. 1300, note L. Marino. *Adde* not. J.-M. Bruguière, « Droit à l'oubli numérique des internautes ou... responsabilité civile des moteurs de recherche du fait du référencement ? », *CCE*, mai 2015, n° 5, p. 15 ; R. Perray et P. Salen, « La Cour de justice, les moteurs de recherche et le droit "à l'oubli numérique" : une fausse innovation, de vraies questions », *RLDI*, nov. 2014, n° 109, p. 35 ; V.-L. Bénabou et J. Rochfeld, « Les moteurs de recherche, maîtres ou esclaves du droit à l'oubli numérique ? Acte I : Le moteur, facilitateur d'accès, agrégateur d'informations et responsable de traitement autonome », *D.*, 2014, p. 1476 ; N. Martial-Braz et J. Rochfeld, « Les moteurs de recherche, maîtres ou esclaves du droit à l'oubli numérique ? Acte II : le droit à l'oubli numérique, l'éléphant et la vie privée », *D.*, 2014, p.

Les faits soumis à la Cour étaient les suivants. M. Gonzalez, citoyen espagnol, était mentionné dans la presse comme ayant fait l'objet de saisies immobilières pour non-paiement de dettes sociales. La publication annonçait la vente aux enchères qui était sur le point de se tenir. Ces informations avaient d'abord été publiées sur papier, avant d'être diffusées une seconde fois sous forme numérique. Surtout, la publication numérique avait été indexée par le moteur de recherche Google, et se trouvait ainsi portée à l'attention de tout internaute présentant une requête de recherche portant sur les nom et prénom de l'intéressé. M. Gonzalez, embarrassé par une histoire vieille de douze ans, demanda le retrait des publications à la fois du site du quotidien La Vanguardia et du moteur de recherche Google. L'Agence espagnole de protection des données (AEPD) rejeta la réclamation à l'encontre de l'organe de presse, cette publication étant parfaitement licite. En revanche, l'Agence avait exigé de Google qu'il procède au retrait des résultats correspondants dans son moteur de recherche. La Cour devait répondre à un ensemble de questions parfois très techniques sur l'interprétation de la directive 95/46, mais l'essentiel du débat pouvait se résumer ainsi : le recensement puis la présentation d'informations licites dans un moteur de recherche peuvent-ils constituer des actes illicites ? L'idée semble d'abord incongrue. C'est pourtant en ce sens que juge la CJUE.

*[...] un traitement de données à caractère personnel, tel que celui en cause au principal, réalisé par l'exploitant d'un moteur de recherche, est susceptible d'affecter significativement les droits fondamentaux au respect de la vie privée et à la protection des données à caractère personnel lorsque la recherche à l'aide de ce moteur est effectuée à partir du nom d'une personne physique, dès lors que ledit traitement permet à tout internaute d'obtenir par la liste de résultats un aperçu structuré des informations relatives à cette personne trouvables sur Internet, qui touchent potentiellement à une multitude d'aspects de sa vie privée et qui, sans ledit moteur de recherche, n'auraient pas ou seulement que très difficilement pu être interconnectées, et ainsi d'établir un profil plus ou moins détaillé de celle-ci. En outre, l'effet de l'ingérence dans lesdits droits de la personne concernée se trouve démultiplié en raison du rôle important que jouent Internet et les moteurs de recherche dans la société moderne, lesquels confèrent aux informations contenues dans une telle liste de résultats un caractère ubiquitaire [...]*³³⁴.

105. Les spécificités de la recherche nominative - La CJUE le souligne à raison : l'information sur les individus est aujourd'hui trop facile à trouver. L'identité numérique, qui pourrait sembler être une abstraction, prend corps en quelques instants lorsqu'un moteur de recherche généraliste est mis en œuvre. En présentant des requêtes de recherche nominative, l'utilisateur de ces services construit en un instant autant de « fiches renseignements généraux », dont l'exhaustivité est problématique. Rappelons qu'en 1978, le rapporteur de la loi informatique et libertés craignait les

1481 ; L. Marino, « Comment mettre en œuvre le “droit à l'oubli” numérique ? », *D.*, 2014, p. 1680.

334. - CJUE, 13 mai 2014, arrêt précité, considérant 80.

effets combinés de l'hypermnésie informatique et des interconnexions massives de bases données : « Est-il indispensable qu'on puisse savoir d'un homme de soixante ans qu'il était énurétique à trois ans, qu'il a contracté la coqueluche à huit ans, qu'il a échoué au baccalauréat à seize ans, qu'il a subi une punition durant son service militaire, qu'il a blessé un passant en voiture à vingt-cinq ans, qu'il a été licencié par un employeur à quarante ans et qu'il a subi une intervention chirurgicale à cinquante ans ? »³³⁵. C'est précisément ce que permettent les moteurs de recherche, du moins s'agissant des informations publiquement accessibles sur Internet – qui sont en nombre considérable : ils les aspirent, les rapprochent et les propulsent sur l'écran des résultats, en n'oubliant rien. En plus d'être d'une extrême précision et de remonter sans limites dans le passé, le profil ainsi obtenu ne présentera pas l'apparence d'une biographie telle qu'elle aurait été rédigée par un journaliste, par exemple. Si le public présentait une attirance particulière pour les informations déshonorantes — on ne fait que formuler l'hypothèse — alors la popularité des liens y afférents augmenterait, et conséquemment leur place dans les résultats de recherche.

Toutefois, si l'extrême puissance des moteurs de recherche constitue le soubassement de la décision *Google Spain*, elle peut facilement être retournée contre l'arrêt. Que des informations gênantes, vieilles et dont la pertinence s'est fanée soient placées trop facilement sous le feu de si puissants projecteurs est une source d'inquiétude. Mais l'alternative est de les plonger dans l'obscurité la plus complète. Certes, l'internaute se rendant sur le site de la *Vanguardia* pourrait encore y taper le nom de M. Gonzalez, et trouver ainsi les articles en cause. En effet, l'arrêt ne vise que le « moteur de recherche consistant à trouver des informations publiées ou placées sur Internet par des tiers », ce qui ne vise pas un moteur de recherche interne³³⁶. La visibilité de l'information, dans un tel exemple, n'est que diminuée – très fortement. Mais un certain nombre de pages qui ne bénéficient pas d'un flux important de visiteurs réguliers, comme des blogs personnels, disparaissent de fait si elles ne profitent pas d'une indexation par les grands moteurs. La solution *Google Spain* serait donc inacceptable si elle exigeait que les propos considérés disparaissent des résultats pour toute requête. Ce n'est heureusement pas ce qui est jugé : seules les requêtes nominatives sont visées. Une requête ne comportant pas de nom doit permettre aux pages considérées d'être présentées parmi les résultats.

106. Une délicate balance des intérêts - Ces dernières considérations minorent l'atteinte à la liberté d'expression, mais ne la suppriment pas. Dresser des obstacles entre une information et le

335. - V.supra, n°47.

336. - Dispositif de l'arrêt, 1). Les paragraphes suivants du dispositif font seulement référence au « moteur de recherche », mais cette expression doit sans doute être considérée comme un simple raccourci de la dénomination utilisée dans le 1).

public qui souhaiterait en avoir connaissance, c'est bien restreindre une liberté fondamentale. L'arrêt *Google Spain* se fonde sur les droits d'accès et d'opposition ci-dessus présentés, mais en les sollicitant considérablement³³⁷. Cela n'est acceptable que si l'atteinte est proportionnée, et qu'elle vise à protéger une autre liberté d'égale importance, comme le droit à la vie privée ou le droit à la protection des données à caractère personnel, qui sont explicitement visés³³⁸. La Cour affirme que ces deux droits « prévalent, en principe, non seulement sur l'intérêt économique de l'exploitant du moteur de recherche, mais également sur l'intérêt de ce public à accéder à ladite information lors d'une recherche portant sur le nom de cette personne »³³⁹. Mais elle poursuit : « [...] tel ne serait pas le cas s'il apparaissait, pour des raisons particulières, telles que le rôle joué par ladite personne dans la vie publique, que l'ingérence dans ses droits fondamentaux est justifiée par l'intérêt prépondérant dudit public à avoir, du fait de cette inclusion, accès à l'information en question »³⁴⁰. On imagine en effet quel désastre ce serait si les personnes aspirant à jouer un rôle public pouvaient « faire le ménage » dans les informations en ligne les concernant.

107. **Une police privée de la recherche en ligne** - Mettre plusieurs libertés fondamentales en balance, en tenant compte du critère factuel et flou du rôle dans la vie publique, c'est l'office du juge, ou à tout le moins d'une autorité administrative indépendante. Et pourtant, de fait, c'est l'exploitant du moteur de recherche qui prendra cette décision en première ligne : la CNIL demande aux citoyens de s'adresser à eux en première intention, quitte à lui présenter ensuite une plainte s'ils ne sont pas satisfaits de la réaction des Google et autres Bing³⁴¹. Ces sociétés sont ainsi investies — malgré elles — d'une fonction de police privée qui ne lasse pas d'inquiéter. Lorsque le moteur refuse de déréférencier, il est probable que la personne ayant formé la demande saisira ensuite la CNIL, car ce recours est facile et gratuit. L'autorité appliquera alors les « critères communs » qu'elle a adoptés avec ses homologues européennes³⁴². On peut certes craindre que la procédure s'arrête là, que les décisions de la CNIL ne soient que rarement frappées d'un recours devant le juge

337. - L'art. 12 de la directive 95/46, cité dans l'arrêt dispose : « Les États membres garantissent à toute personne concernée le droit d'obtenir du responsable du traitement: (...) b) selon le cas, la rectification, l'effacement ou le verrouillage des données dont le traitement n'est pas conforme à la présente directive, notamment en raison du caractère incomplet ou inexact des données [...] ». Les informations relatives à M. Gonzalez n'étaient ni incomplètes, ni inexactes. Quant à l'article 14 de la même directive, il prévoit : « Les États membres reconnaissent à la personne concernée le droit: a) au moins dans les cas visés à l'article 7 points e) et f), de s'opposer à tout moment, pour des **raisons prépondérantes et légitimes tenant à sa situation particulière**, à ce que des données la concernant fassent l'objet d'un traitement [...] » (souligné par nous).

338. - L'arrêt se fonde en effet également sur les articles 7 et 8 de la Charte des droits fondamentaux.

339. - Point 4) du dispositif.

340. - *Ibid.*

341. - <https://www.cnil.fr/fr/effacer-des-informations-me-concernant-sur-un-moteur-de-recherche>.

342. - https://www.cnil.fr/sites/default/files/typo/document/Droit_au_dereferencement-criteres.pdf.

administratif, les individus étant découragés par le temps et le coût nécessaires au regard de l'intérêt du litige³⁴³. Mais au moins une autorité administrative indépendante se sera-t-elle prononcée.

Une autre inquiétude, moins présente sous la plume des commentateurs, concerne la situation inverse : celle dans laquelle le moteur de recherche accepterait trop facilement les désindexations. La liberté d'expression de l'auteur des propos déréférencés est atteinte, mais la CNIL estime que : « [...] les moteurs de recherche n'ont pas à informer le site à l'origine de la diffusion du contenu »³⁴⁴. Par hypothèse, l'auteur de la demande ayant été satisfait, il partira en silence. Qui sera là pour faire valoir, par exemple, que le rôle public de cet individu n'a pas été suffisamment pris en compte ? Il est donc souhaitable que ces moteurs aient une politique restrictive en matière de déréférencement, pour éviter de nombreuses acceptations silencieuses, dont aucune entité indépendante n'aura pu vérifier le bien-fondé ! Un tel système n'est pas acceptable. La bonne solution serait de porter immédiatement les demandes devant la CNIL, sans passer par les acteurs privés. Encore faudrait-il doter cette institution de moyens suffisants : depuis mai 2014, plus de 700 000 demandes ont été adressées à Google, concernant plus de 1,9 million d'adresses Internet³⁴⁵. L'enjeu démocratique le justifie.

108. Quel rayonnement territorial ? - Le « droit à l'oubli » a suscité une autre difficulté, tenant au champ d'application territorial qu'il convenait de lui conférer. Google avait limité l'effet du déréférencement aux extensions européennes de son moteur de recherche (.fr, es., etc.). Il suffisait donc à un internaute français de se connecter à la version en .com – ce qui ne demandait que quelques clics supplémentaires — pour obtenir des résultats de recherche complets, les pages désindexées dans le cadre de la jurisprudence *Google Spain* apparaissant à nouveau. La formation restreinte de la CNIL a considéré, à juste titre, que « (...) la société part du postulat qu'il existerait autant de traitements liés au service Google Search que d'extensions locales du moteur de recherche, alors qu'il s'agit d'un traitement unique doté de multiples chemins d'accès techniques »³⁴⁶. Mais l'étape suivante de son raisonnement consiste à demander un déréférencement mondial des informations. Cela signifierait qu'un internaute américain, par exemple, voit ses résultats de recherche expurgés par l'effet d'une jurisprudence européenne. Certes, il est par hypothèse en train d'effectuer une recherche nominative sur un citoyen de l'Union, et la CNIL

343. - En ce sens : N. Martial-Braz et J. Rochfeld, « Les moteurs de recherche... », art. préc., n° 8.

344. - « Interprétation commune de l'arrêt de la CJUE » par les CNILs européennes : www.cnil.fr/sites/default/files/typo/document/Droit_au_dereferencement-Interpretation-Arret.pdf.

345. - <http://www.google.com/transparencyreport/removals/europeprivacy/>.

346. - Délibération 2016-054 du 10 mars 2016.

souhaite que la protection de ce citoyen soit effective partout dans le monde³⁴⁷. Mais cela signifie bien, quoi qu'on en dise, que l'Europe demande l'altération du fonctionnement du moteur de recherche hors de son territoire. Imaginons qu'un propos diffamatoire soit mis en ligne : si la condamnation pénale de l'auteur est assortie de la suppression de la page incriminée, cela produira nécessairement un effet mondial – une page ou un fragment qui n'existe plus n'est plus référencé par les moteurs de recherche. Mais la jurisprudence *Google Spain* consiste en une illusion, un tour de passe-passe qui vise à retirer fictivement d'Internet un contenu qui s'y trouve bel et bien. On voit mal comment imposer une telle altération aux internautes d'un pays non européen sans que cela soit admis par sa propre législation. Surtout, il est à craindre que des pressions réciproques soient exercées sur les moteurs de recherche par des pays tiers, cette fois-ci au détriment des Européens. Pourquoi ces pays se priveraient-ils d'exiger l'altération de résultats de recherche, y compris sur les écrans situés dans l'Union, par exemple pour diminuer la visibilité de ses opposants politiques ou d'une minorité ?

Cela semble inexorable : en fonction des législations relatives à la protection des données personnelles, à la vie privée, à la liberté d'expression, mais aussi à la propriété intellectuelle, des équilibres différents seront trouvés dans les différentes régions du monde, des déréférencements différents seront exigés des moteurs de recherche, donnant naissance à autant de reflets distincts d'un Internet unique. Dès lors, la mise en œuvre, qui fut décidée par la société Google, d'un filtrage par adresse IP, semble constituer une solution raisonnable. Si cette adresse indique qu'un internaute consulte le moteur depuis le territoire de l'Union européenne, en utilisant n'importe quelle extension nationale, les résultats de recherche sont expurgés conformément à la jurisprudence *Google Spain*. Si l'internaute se situe hors de l'Union, les résultats sont complets. La CNIL ne s'en satisfait pas, relevant que les citoyens de l'Union peuvent voyager occasionnellement ailleurs dans le monde — certes -, mais aussi maquiller leur adresse IP, en utilisant des techniques déjà présentées³⁴⁸. Cette position semble excessive. Altérer son adresse IP — ne parlons même pas de la possibilité de quitter physiquement l'Union européenne — est une démarche que bien peu d'internautes prendront la peine d'effectuer, et qui rend la consultation de résultats de recherche *fastidieuse*. Dans l'hypothèse de propos cibles licites, tout ce contre quoi s'élevait la CJUE était la trop grande facilité avec laquelle ils étaient associés au nom. Il est vrai que les instruments d'altération de l'adresse IP risquent de se démocratiser à l'avenir, mais cela posera des problèmes de régulation et de souveraineté étatique qui dépassent de loin la jurisprudence *Google Spain*. À

347. - « (...) seul un déréférencement sur l'ensemble du moteur de recherche est de nature à permettre une protection effective des droits des personnes » (même délibération).

348. - Délibération 2016-054 précitée. Sur les techniques visant à occulter l'adresse IP, V.supra, n°88.

l'heure actuelle, les obstacles placés sur le chemin de l'internaute paraissent suffisants, et la position des CNIL visant à imposer au reste du monde la vision européenne d'un moteur de recherche licite, excessive.

109. Cas particulier des mineurs – Les auteurs du règlement de 2016 ont manqué de courage s'agissant du droit à l'oubli, reconduisant certes les dispositions de la directive de 1995 ayant servi de fondement à Google Spain, mais sans prendre position directement sur cette importante jurisprudence – que ce soit pour la conforter ou pour la briser. Le règlement n'a innové qu'en ce qu'il accorde aux individus un droit à l'effacement de leurs données personnelles collectées lorsqu'ils étaient mineurs de seize ans, sans qu'ils aient à justifier d'un motif³⁴⁹. En droit interne, la loi République numérique a prévu une mesure similaire, applicable quant à elle aux mineurs de dix-huit ans³⁵⁰. La loi californienne prévoyait un tel droit depuis 2013³⁵¹.

110. Un futur arrêt « Google Spain 2 » ? - Le législateur européen ayant laissé passer l'occasion de préciser les contours du droit au déréférencement, la Cour de justice de l'Union européenne devra poursuivre seule sa construction prétorienne. Saisi d'un recours contre quatre décisions de la CNIL en la matière, le Conseil d'État a en effet estimé qu'il n'était pas en mesure de trancher sans avoir posé préalablement un ensemble de questions préjudicielles à la Cour de Luxembourg³⁵².

d - Le droit de récupérer ses données

111. De l'accès à la récupération - La loi République numérique a inséré dans le Code de la consommation une nouvelle subdivision intitulée « récupération et portabilité des données » - dont l'entrée en vigueur est différée au 25 mai 2018³⁵³. Le futur article L224-42-1 proclame solennellement : « Le consommateur dispose en toutes circonstances d'un droit de récupération de l'ensemble de ses données ». De quoi s'agit-il ? L'individu dispose déjà depuis 1978 d'un droit d'accès à ses données, qui lui permet non seulement de vérifier qu'un responsable de traitement donné dispose d'informations le concernant, mais aussi et surtout d'en connaître la teneur et d'en

349. - L'art. 17 du règlement 2016/679 précité, intitulé « droit à l'effacement », vise notamment : « f) les données à caractère personnel ont été collectées dans le cadre de l'offre de services de la société de l'information visée à l'article 8, paragraphe 1 ». Or ce texte est celui qui requiert le consentement des parents pour les données concernant les enfants de moins de seize ans.

350. - Art. 40, II de la loi 78-17 précitée, issue de l'art. 60 de la loi 2016-1321 précitée.

351. - *Senate Bill* n° 568, consultable sur [leginfo.legislature.ca.gov](http://leginfo.ca.gov) et modifiant le *Business and Professions Codes*, division 8, pour y introduire un nouveau chapitre 22.1.

352. - CE, 24 février 2017, *Mme C, M. F, M. H, M. D.*

353. - Art. L. 224-42-1 et s. C. conso., issus de l'art. 48 de la loi 2016-1321 précitée.

obtenir copie³⁵⁴. Cela ne revient-il pas à « récupérer » lesdites données ? Les deux droits ont des finalités très différentes, qui appellent des modalités techniques de mise en œuvre bien distinctes. Le droit d'accès est le premier d'une série d'outils qui visent à surveiller les responsables de traitement. La personne qui l'exerce procède à une forme d'inspection, qui la renseigne sur l'identité de ceux qui possèdent des parcelles de son intimité, sur l'étendue et l'exactitude des informations détenues, sur la licéité et le fondement du traitement. La personne lutte pour apercevoir de loin ces fragments d'elle-même, qui ont été aspirés par d'autres et sont détenus dans leurs coffres. L'approche est essentiellement défensive. Or, c'est l'un des apports du concept d'autodétermination informationnelle que de revendiquer le droit, pour les individus, d'agir plutôt que de subir ; que de leur reconnaître des moyens de construire, et non seulement d'empêcher. Le droit à la récupération des données vise dès lors à ramener les données personnelles dans le giron de la personne de laquelle elles émanent, à des fins non de contrôle, mais de disposition. Ce pouvoir qui lui est conféré, l'individu peut en user de deux manières : pour sortir d'une situation de dépendance à un prestataire qui gèrait ses données ; pour décider d'appliquer des traitements différents et nouveaux à ses données dans son propre intérêt.

112. La portabilité des données - Lorsqu'un utilisateur de service possède des milliers de photographies, d'emails, de prises de notes stockés auprès d'un prestataire donné, il peut être dissuadé de céder aux sirènes de la concurrence s'il n'est pas en mesure de transporter, chez ce nouveau partenaire, l'ensemble de son capital numérique. Imaginons que le téléchargement de photos soit possible, au sein d'un catalogue en comprenant 5000, mais seulement fichier par fichier. Des centaines d'heures de travail seraient nécessaires à la migration. Le même problème pourrait se poser pour des emails qu'il faudrait copier-coller ou transférer un par un. Le droit d'accès ne constitue pas une réponse à ces difficultés : dans les exemples donnés, le prestataire actuel aurait beau jeu de répondre que la personne peut déjà les consulter dans le cadre normal du service. De plus, le responsable de traitement pourrait, dans le cadre du droit d'accès, fournir le contenu des données sous une forme qui ne permet pas leur exploitation : tirages papier ou formats de fichiers permettant uniquement une consultation passive.

Le règlement de 2016 consacre par conséquent un nouveau « droit à la portabilité des données ». « Les personnes concernées ont le droit de recevoir les données à caractère personnel les concernant qu'elles ont fournies à un responsable du traitement, dans un format structuré, couramment utilisé et lisible par machine, et ont le droit de transmettre ces données à un autre responsable du traitement sans que le responsable du traitement auquel les données à caractère personnel ont été

354. - V.supra, n°100.

communiquées y fasse obstacle [...] »³⁵⁵. Mieux encore, « lorsque cela est techniquement possible », la personne doit pouvoir ordonner le transfert direct de son ancien à son nouveau prestataire³⁵⁶. Certaines conditions sont posées, qui visent essentiellement à restreindre ce droit aux cas de traitement fondés sur le consentement³⁵⁷. L'ambition est claire : il s'agit de fluidifier le marché en s'inspirant par exemple de la « portabilité » des numéros en matière de téléphonie fixe et mobile. Le passage à la concurrence est rendu le plus indolore possible pour le client.

Alors que le règlement de 2016 ne concerne que les données à caractère personnel, la réforme précitée issue de la loi République numérique prévoyait un dispositif distinct visant plus largement « l'ensemble des données », mais ne concernant que les consommateurs, et s'inscrivant dans une partie du Code de la consommation consacrée aux « contrats de services de communications électroniques »³⁵⁸. Surtout, ces règles de droit interne ne devaient s'appliquer qu'à des prestataires ayant atteint une certaine taille critique fixée par décret³⁵⁹. Les champs d'application ne se recoupaient donc pas. Cette dissonance a déplu aux députés du groupe majoritaire : à l'occasion de la discussion de la loi de 2018 relative à la protection des données personnelles, ils ont supprimé le dispositif français pour laisser place au seul mécanisme européen³⁶⁰.

Relevons encore qu'une proposition de directive « sur certains aspects des contrats de fourniture de contenu numérique » envisage de consacrer un droit à la portabilité dont les modalités seraient nettement différentes, puisqu'il naîtrait dans le chef des consommateurs à l'occasion de certaines ruptures de contrats³⁶¹.

Il faut avoir conscience que cette portabilité des données, destinée à stimuler la concurrence, ne fonctionne que dans les situations de tête-à-tête entre la personne dont les données sont collectées et le prestataire qui les exploite. Elle est inefficace face aux très nombreuses plateformes offrant des

355. - Art. 20, 1) du règlement 2016/679 précité.

356. - Art. 20, 2) du même texte.

357. - « a) le traitement est fondé sur le consentement en application de l'article 6, paragraphe 1, point a), ou de l'article 9, paragraphe 2, point a), ou sur un contrat en application de l'article 6, paragraphe 1, point b); et b) le traitement est effectué à l'aide de procédés automatisés » (art. 20 du règlement 2016/679 précité).

358. - Futur art. L. 224-42-1 C. conso.

359. - Futur art. L. 224-42-4 C. conso. : « La présente sous-section ne s'applique pas aux fournisseurs d'un service de communication au public en ligne dont le nombre de comptes d'utilisateurs ayant fait l'objet d'une connexion au cours des six derniers mois est inférieur à un seuil fixé par décret ».

360. - Article 33 de la loi n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles, issu d'un amendement présenté à l'Assemblée nationale (<http://www.assemblee-nationale.fr/15/amendements/0592/AN/155.asp>).

361. - Proposition de directive du Parlement européen et du Conseil concernant certains aspects des contrats de fourniture de contenu numérique du 9 décembre 2015. Sur ce projet, V. not. C. Berthet, C. Zolynski, N. Anciaux et P. Pucheral, « Contenus numériques, récupération des données et empouvoirement du consommateur », *Dalloz IP/IT*, 2017, p. 29.

fonctions — primaires ou même secondaires — de réseau social : il ne sert à rien de disposer de l'ensemble de ses publications sur Facebook pour les importer dans Google + si le réseau d'amis est perdu lors de la migration³⁶².

113. L'utilisation personnelle des données à d'autres fins - Alors que le texte du règlement de 2016 est intitulé « droit à la portabilité des données », le Code de la consommation français vise plus largement « récupération et portabilité ». Et il est vrai que la portabilité n'est que l'un des usages possibles des données récupérées. Ainsi, les promoteurs du « self data » étudient « la production, l'exploitation et le partage de données personnelles par les individus, sous leur contrôle et à leurs propres fins : pour mieux se connaître, prendre de meilleures décisions, évaluer ses décisions passées, se faciliter la vie... »³⁶³. L'idée est la suivante : une fois les données obtenues dans un format compréhensible par les machines, l'individu peut fort bien conserver sa confiance au prestataire qui les lui a livrées, mais tirer un nouveau parti de ses données, seul ou à l'aide d'un partenaire dont l'activité, les modes de traitement et les finalités diffèrent de ceux du prestataire initial. Par exemple, les données rapatriées depuis les logiciels d'aide à la navigation permettront la création de différentes cartes permettant à l'individu d'étudier ses déplacements passés³⁶⁴ ; les données de consommation, issues des moyens de paiement ou cartes de fidélité de supermarché, permettent de calculer son empreinte carbone³⁶⁵ ou de prendre conscience de ses habitudes alimentaires³⁶⁶.

Que le règlement général n'ait pas expressément envisagé la récupération des données à ces fins n'est pas un obstacle insurmontable : il est suffisant qu'il consacre un droit à recevoir ses données dans un format lisible par machine. Mais le risque est que les acteurs de terrain aient interprété ce texte à la lumière de sa finalité de mise en concurrence. Prenons un exemple : quelle chaîne de supermarchés se sera préparée à délivrer les données issues des cartes de fidélité dans un format exploitable par une machine ? Cela n'est pas nécessaire au client qui voudrait faire ses achats ailleurs, mais c'est une ressource précieuse pour celui qui cherche à exploiter lui-même ses données à toutes sortes de fins qu'il juge bonnes. Ce droit, théoriquement acquis devra, donc en pratique être conquis.

362. - V. déjàsupra, n°81.

363. - <http://mesinfos.fing.org/projet/>. La Fing se présente comme « un think tank de nouvelle génération qui aide les entreprises, les institutions et les territoires à anticiper les mutations liées aux technologies et à leurs usages ». Parmi les partenaires de ce projet, sont cités la CNIL, des assureurs, des banques ou encore un moteur de recherche français (<http://mesinfos.fing.org/partenaires/>).

364. - <http://mesinfos.fing.org/mesinfos-geographiques/>.

365. - <http://mesinfos.fing.org/begreen/>.

366. - <http://mesinfos.fing.org/care/>.

Ayant ainsi décrit ce que signifie disposer des données de son vivant, il nous reste à évoquer la disposition à cause de mort.

e – Le droit de transmettre ou non ses données après sa mort

114. La situation antérieure à la loi République numérique - Que deviennent les données à caractère personnel après la mort ? Alors que les textes européens, et notamment le règlement de 2016, se désintéressent de la question, la loi « République numérique » a posé plusieurs règles en la matière³⁶⁷. Avant l'adoption de ce texte, les héritiers se voyaient reconnaître un droit propre, d'ambition limitée et ainsi conçu³⁶⁸ :

Les héritiers d'une personne décédée justifiant de leur identité peuvent, si des éléments portés à leur connaissance leur laissent présumer que les données à caractère personnel la concernant faisant l'objet d'un traitement n'ont pas été actualisées, exiger du responsable de ce traitement qu'il prenne en considération le décès et procède aux mises à jour qui doivent en être la conséquence.

Lorsque les héritiers en font la demande, le responsable du traitement doit justifier, sans frais pour le demandeur, qu'il a procédé aux opérations exigées en vertu de l'alinéa précédent³⁶⁹.

Le défunt laisse en effet derrière lui un avatar numérique, dont la persistance peut laisser croire — à tort — que la personne qu'il représente est toujours en vie. Des comptes sur les réseaux sociaux, un blog personnel resteront accessibles aux tiers au-delà du trépas, et seront référencés par les moteurs de recherche. Bien sûr, aucun nouveau message de l'utilisateur n'apparaîtra - à moins qu'il n'ait prévu des publications à effet différé, ce qui n'est pas rare en matière de blogs. Mais ses connaissances ignorant sa disparition continueront peut-être à alimenter les espaces qui leur sont accessibles, comme un « mur » Facebook ou un espace de commentaires sous un article, nourrissant l'illusion de vie. Le texte ci-dessus reproduit constituait, dès avant la loi République numérique, un fondement donné aux héritiers pour obtenir la fermeture de ces espaces en ligne, ou l'insertion d'une mention informant les visiteurs du décès de l'individu. Facebook permet par exemple la transformation d'un profil d'utilisateur en un « compte de commémoration »³⁷⁰. La CNIL souligne

367. - Art. 40-1 de la loi n° 78-17 précitée issu de l'art. 63 de la loi n° 2016-1321 précitée.

368. - Mentionnons ici les études consacrées à la « mort numérique » antérieures à la réforme de 2016 : V. not. C. Béguin-Faynel, « Pour un testament des dernières volontés numériques », in *Traité des nouveaux droits de la mort. La Mort, incarnation(s) cadavérique(s)*, dir. M. Touzeil-Divina, M. Bouteille-Brigant et J.-F. Boudet, éd. L'Épître, 2014, chap V, section 3 ; A. Mâzouz, « Être ou ne plus être ? Les volontés à l'origine de la mort numérique », in *Droit et réseaux sociaux*, dir. V. Ndior, éd. LEJEP, 2016, p. 183.

369. - Art. 40 de la loi 78-17 dans sa rédaction antérieure à la loi n° 2016-1321, al. 6 et 7.

370. - V. la présentation de cette fonctionnalité par le réseau social : <http://fr-fr.facebook.com/help/contact/651319028315841>.

l'enjeu d'une telle fonctionnalité en précisant que sur ce réseau social, « un profil sur cent serait celui d'une personne décédée, soit environ 13 millions de profils ! »³⁷¹.

Apporter la nouvelle de la mort dans les espaces de vie numériques, permettre le dépôt de couronnes mortuaires virtuelles, tout cela est important, mais n'épuise pas la question de la « mort numérique ». Les héritiers pourront-ils accéder aux données personnelles non publiques ? Les coffres des responsables de traitement sont bourrés d'informations sur le défunt, dont l'intérêt économique ou moral peut être majeur. « Accéder aux données personnelles » du mort c'est ouvrir ses relevés de comptes bancaires et ses déclarations fiscales, sa correspondance professionnelle, amicale, amoureuse, adultère, un agenda pouvant s'étendre sur des décennies, un album de photographies contenant peut-être des centaines de milliers de clichés, son répertoire téléphonique, le relevé de ses localisations géographiques. Dans ce très vaste ensemble, on imagine que des informations sont indispensables à ses associés pour le bon fonctionnement de la société dont il était le fondateur ; que tous les moments importants de la vie de famille ont été immortalisés par ses soins, féru qu'il était de photographie, de sorte que ces souvenirs irremplaçables seront perdus pour tous si l'accès y est refusé ; que son conjoint survivant a besoin de pièces administratives numérisées et stockées sur un serveur distant pour faire valoir ses droits à une pension de réversion. Les raisons d'offrir aux héritiers un accès aux données ne manquent pas. Mais des raisons tout aussi impérieuses pourraient s'y opposer : c'est toute l'intimité du défunt qui pourrait être mise à nu, le moindre de ses secrets qui pourrait être révélé.

Comment trancher ce difficile débat ? Les textes antérieurs n'offraient pas de solution d'ensemble³⁷². La loi République numérique constitue donc un progrès.

115. Le respect des directives anticipées - Le nouvel article 40-1 de la loi informatique et libertés s'ouvre sur un principe clair : les droits octroyés à la personne pour le contrôle de ses données à caractère personnel « s'éteignent au décès de leur titulaire »³⁷³. Puisque le droit de l'individu sur ses informations relève de la sphère des droits de la personnalité, la solution est

371. - CNIL, *Mort numérique : peut-on demander l'effacement des informations d'une personne décédée ?*, publication du 29/10/14 (<https://www.cnil.fr/fr/mort-numerique-peut-demander-leffacement-des-informations-dune-personne-decedee-0>).

372. - Comme le relève M. Luc Belot, rapporteur de la loi République numérique pour l'Assemblée Nationale (rapport n° 3399, consultable sur le site de l'Assemblée), le droit d'accès aux données personnelles de la loi informatiques et libertés a pu être interprété par le Conseil d'État comme appartenant aux héritiers, en tant qu'ils visent « toute personne » pour les données « la concernant », les ayant droits étant alors des personnes concernées (CE, 29 juin 2011, n° 339147). La décision concernait le fichier Fichiers national des comptes bancaires et assimilés (FICOBA). Le rapporteur cite encore l'article L1110-4, V, al. 3 du Code de la santé publique : « Le secret médical ne fait pas obstacle à ce que les informations concernant une personne décédée soient délivrées à ses ayants droit [...] ».

373. - Article 40-1 de la loi n° 78-17 précitée.

cohérente³⁷⁴. Mais la suite du texte surprend alors : « Toutefois, [ces droits] peuvent être provisoirement maintenus conformément aux II et III suivants ». Les héritiers bénéficient peut-être, dans certaines situations, de prérogatives *semblables* à celles que possédait le défunt. Mais cela signifie que la loi fait naître des droits nouveaux qui leur sont *propres*, simplement moulés, dans leur diversité et leur étendue, sur ceux que l'on reconnaît à une personne vivante. En effet, le droit au respect de la vie privée et le droit à l'image — dont le droit sur les données personnelles semble être un proche cousin — s'éteignent à la mort de leur titulaire, comme cela a été clairement jugé par la Cour de cassation³⁷⁵.

Quoi qu'il en soit, pour savoir s'il convient de conférer à des proches du défunt des pouvoirs sur ses données personnelles, la loi commande de respecter les directives qu'il aurait pu formuler à ce propos. Plus précisément, le texte envisage des instructions de l'individu « relatives à la conservation, à l'effacement et à la communication de ses données à caractère personnel après son décès »³⁷⁶. Le *de cuius* peut donc choisir de transmettre, mais aussi de détruire. En prévoyant l'existence de directives générales — confiées à un « tiers de confiance numérique » certifié par la CNIL — mais aussi de directives particulières — adressées directement au responsable de traitement concerné -, la loi promeut le rôle de la volonté dans la gestion de l'au-delà numérique et propose une gestion fine, discriminant selon les contenus et les prestataires. En pratique, le notariat se positionnera rapidement comme le « tiers de confiance » naturel en matière de directives générales, et ne manquera pas de formuler des conseils concernant le sort des données lors de la rédaction de testaments authentiques. L'analogie testamentaire est d'ailleurs développée par le texte de la loi, qui prévoit la possibilité de désigner une personne chargée de l'exécution des directives post-mortem³⁷⁷. Quant aux directives particulières, la pratique de la société Google — antérieure à l'adoption de la loi — en fournit un exemple. Un « gestionnaire de compte inactif » est proposé aux utilisateurs³⁷⁸. Après une période pudiquement qualifiée de « période d'inactivité » — d'un minimum de trois mois, et durant laquelle aucune connexion au compte n'aura été enregistrée — il est possible d'octroyer à un ou plusieurs « contacts de confiance » un accès à tout ou partie de ses données personnelles. Par exemple, un ami pourra accéder exclusivement aux photos, tandis que le conjoint pourra à la fois regarder les photographies et lire les emails.

374. - V.supra, n°96.

375. - V. not. Cass. 1ère civ., 15 févr. 2005, n° 03-18.302 : « [...] le droit d'agir pour le respect de la vie privée ou de l'image s'éteint au décès de la personne concernée, seule titulaire de ce droit [...] ».

376. - Art. 40-1, II de la loi n° 78-17 précitée. L'ensemble de ce II est d'ordre public, ainsi qu'il est précisé *in fine*.

377. - Même texte.

378. - <https://support.google.com/accounts/answer/3036546?hl=fr>.

Comment critiquer cette partie de la loi ? Comment refuser au principal intéressé la maîtrise de ses « cendres numériques » ? Il est probable que l'adoption de telles directives entrera peu à peu dans les mœurs des générations ayant grandi avec les nouvelles technologies de l'information et de la communication. La loi prévoit d'ailleurs que : « Tout prestataire d'un service de communication au public en ligne informe l'utilisateur du sort des données qui le concernent à son décès et lui permet de choisir de communiquer ou non ses données à un tiers qu'il désigne ». À l'heure actuelle, de telles consignes sont rares et leur absence restera longtemps la norme. Le contenu de la loi supplétive de volonté est donc d'une importance capitale.

116. En l'absence de directives : les hésitations des parlementaires - Si le défunt ne s'est pas prononcé, faut-il fermer à ses proches l'accès à ses données personnelles, ou l'ouvrir largement, ou l'ouvrir un peu ? L'Assemblée nationale et le Sénat ont adopté des approches opposées, sur lesquelles il est utile de revenir brièvement, car elles sont riches d'enseignement sur la manière dont la « mort numérique » est perçue par ceux qui font la loi. Le Gouvernement lui-même n'a pas montré un cap très précis. Dans le projet de loi initial, il était en effet prévu : « Sauf lorsque la personne concernée a exprimé une volonté contraire [...], ou en l'absence de directives, ses héritiers, dans l'ordre mentionné au précédent alinéa, peuvent exercer après son décès les droits mentionnés à la présente section »³⁷⁹. Devant la commission des lois de l'Assemblée, le Gouvernement se ravise et présente un amendement supprimant la transmission automatique aux héritiers des droits « informatique et libertés » en l'absence de directive³⁸⁰. Il suit en cela l'avis formulé par la CNIL, qui considère :

*[...] que la faculté pour un héritier d'accéder aux données du défunt devrait être assortie de conditions strictes et de garanties pour préserver la mémoire du défunt et des tiers. Il pourrait notamment être envisagé de prévoir l'accès aux données contenues dans des traitements lorsqu'un tel accès est nécessaire pour identifier l'actif successoral d'une personne, ou lorsque l'impossibilité d'accès cause un préjudice réel, direct et certain aux héritiers*³⁸¹.

C'est ainsi que le texte adopté par l'Assemblée nationale prévoit qu'« en l'absence de directives, les droits mentionnés à la présente section s'éteignent avec le décès de leur titulaire », mais retient la première dérogation suggérée par la CNIL, lorsque les données sont nécessaires à la liquidation et au partage de la succession³⁸².

379. - Article 32, avant-dernier alinéa du projet de loi pour une République numérique, n° 3318.

380. - Amendement n° CL687.

381. - CNIL, *Délibération n° 2015-414 du 19 novembre 2015 portant avis sur un projet de la loi pour une République numérique*, p. 18.

382. - Article 32 du texte adopté à l'Assemblée nationale en première lecture.

Cependant, la Commission des lois du Sénat va revenir à l'état premier du texte, et ainsi redonner aux héritiers un accès automatique aux données personnelles du défunt, en l'absence de directive anticipée³⁸³. En séance plénière, des sénateurs proposent de revenir à la position adoptée par l'Assemblée nationale et le rapporteur de la Commission des lois du Sénat, M. Christophe-André Frassa, a l'occasion d'expliquer pourquoi il s'y oppose.

Le dispositif proposé [...] crée une césure complète entre la succession numérique et la succession physique. Alors que, dans le monde physique, il appartient à chacun de protéger, par anticipation, ses secrets, dans le monde numérique, le principe serait celui du secret.

Les difficultés pratiques posées par ce dispositif sont nombreuses : par exemple, si le défunt a stocké ses photos de famille sur le nuage — le cloud —, les héritiers n'y auront plus accès, alors que, dans une succession physique, le partage des albums de famille est, bien entendu, possible. De la même manière, le courrier électronique sera inaccessible, alors que les courriers papier sont remis sans problème aux héritiers.[...]

Les dérogations prévues en faveur des héritiers seront largement ineffectives : pour demander à accéder à une donnée personnelle susceptible d'être nécessaire pour la liquidation de la succession, encore faut-il savoir que cette donnée existe, ce qui nécessite de pouvoir consulter plus largement le traitement, afin d'identifier ce qui peut être utile. Or les héritiers n'auront pas le droit de procéder à cette consultation plus large... [...]

J'ajoute, enfin, que se pose aussi la question du devenir des biens numériques : faut-il estimer que la propriété cesse à la mort de l'intéressé et que rien ne passe alors aux héritiers ?[...] ³⁸⁴.

D'autres intervenants vont mobiliser l'analogie entre « succession numérique » et « succession physique ». Ainsi M. Bas, président de la Commission des lois du Sénat, affirme-t-il :

La règle veut que, à notre décès, tout secret que nous n'avons pas confiné de telle manière que nul ne puisse y accéder soit accessible à nos héritiers. Je ne vois pas pourquoi cette règle pourrait être modifiée pour les seuls secrets conservés sur Internet et maintenue, en revanche, pour ceux qui le seraient sur des supports différents des supports électroniques. Il n'y a strictement aucune raison tenant aux droits fondamentaux de la personne d'introduire cette différenciation ³⁸⁵.

L'argument finira par être désigné, en raccourci, comme celui de la « boîte à chaussures », en référence aux trésors que tout héritier est susceptible de retrouver dans le grenier du défunt, personne ne contestant alors que les cartes postales, photographies ou lettres manuscrites s'y trouvant peuvent être consultées. La métaphore est fallacieuse, pour deux raisons au moins.

383. - Amendement COM-299 proposé par M. Christophe-André Frassa, et adopté contre l'avis du Gouvernement.

384. - Compte-rendu intégral des débats du 29 avril 2016.

385. - *Ibid.*

D'abord, l'analogie suppose que les données personnelles soient librement accessibles, comme l'est le contenu de la boîte à chaussures. Ce serait le cas si le *de cujus* avait communiqué ses identifiant et mot de passe à ses proches, ou s'il les avait inscrits sur un morceau de papier rangé dans un tiroir ou collé sur son écran d'ordinateur. Ce serait encore le cas si ces mots de passe étaient préremplis par son navigateur Internet, de sorte que toute personne prenant possession du clavier pourrait accéder à son compte. Par hypothèse, dans toutes ces situations, il n'est pas nécessaire d'enjoindre au responsable de traitement d'ouvrir un accès aux héritiers, en invoquant la force de la loi, puisqu'ils disposent déjà d'une maîtrise de fait sur les données. Ce sont les autres situations que le législateur doit saisir. La boîte à chaussures serait alors assortie d'un verrou impossible à crocheter.

Ensuite et surtout, le raisonnement proposé repose sur une prémisse inexacte. Si l'on ne voit pas pourquoi il faudrait traiter différemment « succession physique » et « succession numérique », c'est parce que les données personnelles ne sont pas des biens, et qu'ils ne font par conséquent l'objet d'aucune dévolution successorale³⁸⁶. La CNIL l'avait rappelé³⁸⁷. En revanche, les véritables « biens numériques » auxquels M. Frassa fait allusion, notamment des copies immatérielles de films, de disques, de logiciels devraient il est vrai être transmis aux héritiers, comme cela sera démontré plus loin - mais il s'agit d'une tout autre question³⁸⁸.

117. En l'absence de directives : la solution retenue - Peu rigoureuse sur le plan juridique, la solution promue au Sénat était de surcroît inopportune, en offrant aux héritiers un accès sans nuance à l'océan des données personnelles de toute personne n'ayant pas laissé de directive particulière en la matière. On pourrait donc se réjouir qu'après la réunion d'une commission mixte paritaire, le texte soit revenu à une non-transmission de principe, assortie d'exceptions. Mais l'enthousiasme serait de courte durée, tant la mise en œuvre d'une de ces exceptions présente de dangers. La loi dispose que :

En l'absence de directives ou de mention contraire dans lesdites directives, les héritiers de la personne concernée peuvent exercer après son décès les droits mentionnés à la présente section dans la mesure nécessaire :

386. - La Secrétaire d'État au numérique objectait : «[...] je considère que la boîte à chaussures que l'on retrouvait dans le grenier du défunt n'équivaut pas à ce que l'on trouve dans le nuage informatique – le cloud. À moins que la boîte à chaussures n'ait les dimensions d'un container maritime ». Mais il y a bien une différence de nature, et pas seulement de degré.

387. - « [...] les droits visés par le projet de loi sont des droits personnels qui disparaissent à la mort de la personne (droits d'opposition, d'accès, d'effacement, de rectification). Si la dévolution des droits réels peut intervenir automatiquement selon les règles successorales prévues par le code civil, l'exercice des droits personnels reconnus par la loi dépend avant tout de la volonté de leur titulaire » (délibération n° 2015-414 précitée, p. 17).

388. - V.infra, n° 125 et s.

[...] à la prise en compte, par les responsables de traitement, de son décès. À ce titre, les héritiers peuvent faire procéder à la clôture des comptes utilisateurs du défunt, s'opposer à la poursuite des traitements de données à caractère personnel le concernant ou faire procéder à leur mise à jour³⁸⁹.

Il ne s'est agi ici que de reprendre le dispositif qui préexistait à la loi République numérique, en le précisant un peu - ainsi de la référence nouvelle à la « clôture des comptes utilisateurs »³⁹⁰. Le problème n'est donc pas là. Mais la loi vise également l'exercice des droits du défunt dans la mesure nécessaire

[...] à l'organisation et au règlement de la succession du défunt. À ce titre, les héritiers peuvent accéder aux traitements de données à caractère personnel qui le concernent afin d'identifier et d'obtenir communication des informations utiles à la liquidation et au partage de la succession. Ils peuvent aussi recevoir communication des biens numériques ou des données s'apparentant à des souvenirs de famille, transmissibles aux héritiers.

Laissons de côté l'amalgame déjà évoqué entre « données personnelles » et « biens numériques », deux catégories juridiques qu'il conviendrait au contraire de soigneusement distinguer. L'essentiel n'est pas là. Le législateur imagine ici conférer des droits aux héritiers sur certaines données seulement : celles qui sont nécessaires au règlement de la succession d'une part, et celles qui constituent des souvenirs de famille d'autre part. Encore faut-il trouver ces quelques perles au milieu de l'océan. Si un tiers de confiance, le notaire par exemple, avait été chargé de plonger et de procéder à la récolte, les secrets du défunt auraient été préservés. Ils auraient été indemnisés pour ce travail, qui est certes chronophage, mais pas insurmontable, s'il est sainement conçu : seules des informations dont les héritiers savent *a priori* qu'elles existent et — au moins dans les grandes lignes — en quoi elles consistent, devraient faire l'objet de telles recherches. Or, ce n'est pas la solution retenue par le législateur, qui semble consacrer une liberté totale de se promener dans les informations personnelles du *de cuius*, afin de déterminer soi-même ce qui présente un intérêt. Il faut voir dans cette curieuse procédure des concessions — importantes — des députés aux sénateurs³⁹¹. Le principe selon lequel les héritiers n'ont pas de pouvoir sur les données du défunt en l'absence de directive de sa part semble ainsi totalement vidé de sa substance.

389. - Art. 40-1, III de la loi n° 78-17 précitée.

390. - Sur le texte antérieur, V. *supra*, n°114.

391. - V. les propos de M. Frassa, *supra*, n° 116 : « les dérogations prévues en faveur des héritiers seront largement ineffectives [...] ». Devant la Commission mixte paritaire, le député M. Belot déclare : « La proposition de rédaction n° 8 relative à la “mort numérique” s'appuie sur la rédaction du Sénat sous réserve de quelques modifications présentées par mon collègue sénateur qui, je l'espère, satisferont tout le monde ».

L'IDENTITÉ NUMÉRIQUE : CONCLUSION

L'identité peut être définie comme l'image sociale d'une personne, construite concurremment par l'individu lui-même et par les tiers. Selon les situations, les publics, les contextes, elle fait l'objet de révélations dont l'étendue varie considérablement. Pour l'accomplissement de certaines démarches administratives, pour la conclusion de contrats, lorsqu'il s'agit de recevoir une peine ou une récompense, des preuves solides de l'identité doivent être fournies : elles permettront au système juridique de créditer ou de débiter le bon compte, parmi l'ensemble des individus dont il encadre l'existence. Dans d'autres situations, l'identité doit au contraire être préservée contre des curiosités déplacées : la vie privée, l'honneur, l'intime méritent de fermes protections.

Ces différents enjeux ne datent pas d'Internet, mais ils sont exacerbés par le numérique. Le réseau fait cohabiter les anonymats les plus épais avec les registres les plus impudiques et les plus exhaustifs qui soient sur la vie secrète des individus. Le spectre de l'identité semble avoir été élargi par le numérique, et rendu plus dense à ses extrémités. Le droit ne peut rester sans réagir.

Mais toutes ces questions sont-elles bien liées ? L'identification et la protection de l'intime ne se trouvent-elles pas rassemblées par la simple polysémie trompeuse du mot « identité » ? La cohérence existe bel et bien. Deux « identités » sont déclinées dans l'étude qui, sur Internet, sont profondément liées l'une à l'autre : une identité « stable » et une identité « construite ». Entre elles, les allers et retours sont fréquents.

« L'identité stable » désigne les coordonnées sociales uniques, faiblement variables au cours de la vie, qui désignent un et un seul individu au sein d'une société. Par défaut, elle est dissimulée sur Internet, en vertu des choix techniques fondateurs du réseau. Loin d'être toujours un inconvénient, cette situation est parfois un avantage qui doit être protégé. Mais lorsqu'il est nécessaire de prouver qui l'on est, le droit requiert des procédures fiables. Le rôle majeur du chiffrement dans ce processus a été souligné. Ce rappel est indispensable, tant les techniques cryptographiques sont exclusivement associées, dans un certain discours public, à la protection de secrets — nécessairement coupables — alors même qu'elles sont aussi la clé de la transparence et de la confiance en ligne.

« L'identité construite » est le fruit des progrès spectaculaires dans la collecte, le traitement et le recoupement de myriades de fragments d'intimité. Le risque de l'omniscience des bases de données a été perçu dès 1978, mais il a cru depuis lors de manière exponentielle. Au sein des protections érigées par les réglementations française et européenne, ou simplement permises par la technique,

deux masses bien distinctes ont été mises en évidence. La première regroupe les barrières d'ordre public, qui sont déployées sans qu'une initiative particulière soit nécessaire de la part de l'individu protégé. Elles ont été présentées en détail, mais la part d'ineffectivité qu'elles recèlent n'a pas été dissimulée. Ces faiblesses sont en partie imputables à la conception même des règles, en partie aux moyens très insuffisants alloués aux autorités de contrôle. Si un arsenal de sanctions conséquent va être mis à la disposition des autorités de protection des données dès mai 2018, à l'occasion de l'entrée en vigueur d'un nouveau règlement européen, leurs moyens budgétaires et humains sont en effet loin d'être à la hauteur des enjeux. La deuxième masse contient les instruments juridiques et techniques permettant aux individus qui le souhaitent d'aller bien plus loin dans la protection et la gestion de leur avatar numérique. À ce titre, deux avertissements importants ont été formulés. D'abord, l'écrasante majorité des citoyens n'a pas recours à ces outils, faute d'une compétence suffisante pour les manier et, plus radicalement, par inconscience des dangers qui planent sur son intimité numérique. Une formation à ces matières devrait être largement dispensée. Ensuite, ceux qui souhaitent et peuvent recourir à cette gestion avancée de leur représentation dans les bases de données risquent d'en être empêchés par les orientations prises par les législations antiterroristes. Qu'il s'agisse de dissimuler son adresse IP, le contenu de disques durs ou la teneur d'échanges électroniques, un grand nombre de comportements pourtant légitimes sont pointés du doigt par des responsables publics comme suspects. La démonstration a été proposée du caractère irresponsable de leur prohibition, qui n'entraverait en rien les projets des fous ou des criminels, mais laisserait les populations totalement nues sous l'œil des grandes entreprises, des mafias et des services de renseignements du monde entier.

Chapitre 2 - La communication électronique

118. « **Une conversation mondiale sans fin** » - L'étude des données à caractère personnel nous a conduits à aborder à plusieurs reprises, la question des communications électroniques. Ce que l'individu dit aux autres, ce à quoi il tend l'oreille, les échanges d'idées auxquels il prend part, sous forme de texte, mais aussi d'images fixes, de vidéo, de sons, participent profondément de ce qu'il est. Ils devaient donc se rencontrer incidemment dans une étude de ce qui constitue l'identité numérique. Il est temps, toutefois, de faire de la communication notre centre d'intérêt principal, de sortir la personne de l'examen isolé à laquelle nous l'avions soumise, pour la faire entrer en relation avec le monde. Or, Internet est tout entier communication : entre les machines, entre les réseaux et, partant, entre les hommes. Comme tout média, il peut être le support d'expressions qui heurtent des valeurs sociales, parmi les plus essentielles. On peut y inciter à la haine, y dégrader la dignité humaine, y préparer la commission d'actes terroristes ; des honneurs y sont traînés dans la boue, et des sexualités perverses s'y épanouissent. À ce titre, il est amené à devenir la cible constante du législateur. Mais comme tout média, il peut servir l'accès à la culture, le débat d'idées et la contestation du pouvoir politique. Des libertés fondamentales peuvent donc être brandies contre les attaques du Parlement. Si ces tensions ne sont pas nouvelles dans leur principe même, sans doute sont-elles inédites par leur intensité. Internet n'est pas aujourd'hui l'un des supports de communication : il est le plus puissant d'entre tous.

Dès 1997, la Cour suprême des États-Unis eut à examiner une législation fédérale visant à protéger les mineurs des contenus à caractère pornographique³⁹². Une association américaine de défense des libertés publiques estimait qu'elle était contraire au Premier amendement à la Constitution, qui défend le droit à la liberté d'expression³⁹³. L'un des juges du tribunal de district dont la décision était attaquée avait écrit qu'Internet peut être regardé « comme une conversation mondiale sans fin »³⁹⁴. Quant à la Cour suprême, voici comment elle présenta les enjeux de l'affaire qui lui était soumise :

[...] The Web is thus comparable, from the readers' viewpoint, to both a vast library

392. - *Reno v. American Civil Liberties Union*, 521 U.S. 844 (1997).

393. - « *Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the Government for a redress of grievances* ».

394. - Stuart Dalzell écrit : « *The Internet may fairly be regarded as a never-ending worldwide conversation* ». La traduction est celle proposée par le rapport précité du Conseil d'État, *Le numérique et les droits fondamentaux*, p. 90.

including millions of readily available and indexed publications and a sprawling mall offering goods and services.

From the publishers' point of view, it constitutes a vast platform from which to address and hear from a world-wide audience of millions of readers, viewers, researchers, and buyers. Any person or organization with a computer connected to the Internet can "publish" information [...]³⁹⁵.

La Cour précisa que la liberté d'expression devait être protégée de manière plus intense en ligne qu'en matière audiovisuelle, notamment parce que la consultation de sites Internet requiert des démarches positives et peut faire l'objet d'avertissements, alors qu'une émission de radio ou de télévision est subie par le spectateur³⁹⁶.

Deux leçons peuvent être retenues de cette décision américaine, rendue très tôt dans l'histoire du développement grand public d'Internet. D'abord, des différences dans les modes de production ou de consultation de l'information sur les réseaux, par rapport aux médias préexistants, peuvent justifier une réglementation juridique ou des raisonnements particuliers - nous y reviendrons largement. Ensuite, Internet ne peut être décrit comme un mode de communication anodin parmi tous ceux offerts aux citoyens : sa place centrale dans les formes contemporaines d'échanges d'informations confère une gravité particulière aux restrictions qui l'affectent. L'affirmation audacieuse de 1997 est devenue vérité d'évidence douze ans plus tard, lorsque le Conseil constitutionnel français doit se prononcer sur la loi dite Hadopi.

119. La liberté d'accès à Internet - Les Sages examinaient la constitutionnalité d'une loi de 2009, qui créait une nouvelle autorité administrative indépendante destinée à lutter contre la contrefaçon en ligne, et lui confiait le pouvoir de suspendre l'accès à Internet des contrevenants³⁹⁷. Après avoir rappelé les termes de l'article 11 de la Déclaration des droits de l'Homme et du citoyen, consacrant la liberté de communication, le Conseil affirme :

[...] en l'état actuel des moyens de communication et eu égard au développement généralisé des services de communication au public en ligne ainsi qu'à l'importance prise par ces services pour la participation à la vie démocratique et l'expression des idées et des opinions, ce droit implique la liberté d'accéder à ces services [...]³⁹⁸.

395. - Arrêt précité *Reno v. American Civil Liberties Union*.

396. - V. l'analyse du rapport précité du Conseil d'Etat, *Le numérique et les droits fondamentaux*, p. 90. La Cour suprême relève notamment que « [...] the receipt of information on the Internet requires a series of affirmative steps more deliberate and directed than merely turning a dial. A child requires some sophistication and some ability to read to retrieve material and thereby to use the Internet unattended » (reprenant ainsi le *finding* 89 de la *District Court*).

397. - Décision n° 2009-580 DC du 10 juin 2009, rendue à propos de la loi n° 2009-669 du 12 juin 2009 favorisant la diffusion et la protection de la création sur Internet.

398. - Considérant 12.

Le droit d'accès à Internet devient ainsi un appendice du droit à la communication³⁹⁹. Cela ne signifie pas que ce droit est insusceptible de limitation ou de suspension, mais les conditions dans lesquelles ces atteintes avaient été organisées par la loi déferée au Conseil n'étaient pas acceptables. Les actes de contrefaçon constatés sur les réseaux d'échanges de fichiers de pair-à-pair ne laissent apparaître qu'une adresse IP, qui désigne une machine connectée au réseau, et non une personne. Il a déjà été exposé que le législateur avait contourné cette difficulté en faisant peser sur le titulaire de l'accès à Internet une obligation de surveiller l'emploi qui était fait de sa connexion par les utilisateurs légitimes, et la sécurité du point d'accès pour éviter les usages non autorisés⁴⁰⁰. Le dispositif prévu par la loi déferée au Conseil se fondait sur un manquement à cette obligation pour autoriser une autorité administrative à suspendre l'accès au réseau de l'abonné, en présumant sa responsabilité pénale, et sans que la sanction soit prononcée par un juge : ces considérations ont entraîné la censure partielle de la loi⁴⁰¹.

Ainsi la suspension d'accès à titre de mesure répressive ne peut-elle être prononcée que moyennant des garanties procédurales suffisantes. Mais la liberté d'accès à Internet n'est pas seulement protégée en droit pénal : le droit civil s'en préoccupe depuis peu. En 2012, la Deuxième chambre civile de la Cour de cassation avait ainsi rendu un arrêt audacieux. Allant au-delà de la lettre des textes régissant les procédures civiles d'exécution, elle avait jugé que : « (...) un ordinateur utilisé pour la recherche d'un emploi doit être assimilé à un instrument nécessaire à l'exercice personnel d'une activité professionnelle » et qu'à ce titre, il est insaisissable⁴⁰². La Haute juridiction prend appui sur la protection légale des instruments de travail, qu'elle étend au terminal

399. - L. Marino, « Le droit d'accès à Internet, nouveau droit fondamental », *D.*, 2009, p. 2045.

400. - V. *supra*, n°51.

401. - V. spéc. le considérant 16 : « 16. Considérant que les pouvoirs de sanction institués par les dispositions critiquées habilitent la commission de protection des droits, qui n'est pas une juridiction, à restreindre ou à empêcher l'accès à Internet de titulaires d'abonnement ainsi que des personnes qu'ils en font bénéficier ; que la compétence reconnue à cette autorité administrative n'est pas limitée à une catégorie particulière de personnes, mais s'étend à la totalité de la population ; que ses pouvoirs peuvent conduire à restreindre l'exercice, par toute personne, de son droit de s'exprimer et de communiquer librement, notamment depuis son domicile ; que, dans ces conditions, eu égard à la nature de la liberté garantie par l'article 11 de la Déclaration de 1789, le législateur ne pouvait, quelles que soient les garanties encadrant le prononcé des sanctions, confier de tels pouvoirs à une autorité administrative dans le but de protéger les droits des titulaires du droit d'auteur et de droits voisins ».

402. - Cass. 2e civ., 28 juin 2012, n° 11-15.055 : Dr. famille, 2013, n° 9, comm. 113, obs. G. Guerlin. Cet auteur relève que la Cour ne qualifie pas l'ordinateur d'instrument de travail, mais **l'assimile** à un tel instrument pour obtenir un alignement des régimes juridiques. Il ajoute : « Pour comprendre l'arrêt commenté, il n'y a donc pas lieu de tourner indéfiniment autour de la lettre du Code, que la Cour de cassation a outrepassée. C'est davantage l'esprit de la matière qu'il faut envisager, dans un contexte préoccupant de crise économique. La Cour de cassation n'ignore pas qu'un ordinateur peut servir à chercher du travail, à rédiger ou transmettre un curriculum vitae, à répondre à des offres d'emploi ou à communiquer avec le conseiller de Pôle emploi. Elle sait, du reste, que le Conseil constitutionnel protège l'accès à Internet sur le fondement de l'article 11 de la Déclaration des droits de l'homme et du citoyen de 1789 ». V. déjà en 2008 : C. Manara et B. Tabaka, « Pour l'insaisissabilité de l'ordinateur familial », *AJ famille*, 2008, p. 207.

utilisé pour accéder au réseau, en ce qu'il permet — entre autres — les communications à des fins professionnelles. Ce dernier terme est entendu très largement, puisque l'individu concerné était au chômage, mais il est vrai qu'obérer sa capacité à échanger des informations avec le reste du monde diminue ses chances de trouver ou de retrouver un emploi. Dans la mesure, toutefois, où l'outil ainsi préservé n'est pas limité à des échanges d'information à vocation professionnelle, c'est aussi l'accès plus général à des interactions sociales, à la culture et au divertissement des plus pauvres qui est indirectement protégé. Le bouclier jurisprudentiel ainsi érigé devant le terminal serait toutefois de peu d'utilité sans un abonnement fonctionnel à un FAI, dont les indigents risquent d'être privés en cas d'impayés. Mais la récente loi République numérique a réformé le Code de l'action sociale et des familles, qui dispose désormais :

(...) toute personne ou famille éprouvant des difficultés particulières, au regard notamment de son patrimoine, de l'insuffisance de ses ressources ou de ses conditions d'existence, a droit à une aide de la collectivité pour disposer de la fourniture d'eau, d'énergie, d'un service de téléphonie fixe et d'un service d'accès à internet.

En cas de non-paiement des factures, la fourniture d'énergie et d'eau, un service téléphonique et un service d'accès à internet sont maintenus jusqu'à ce qu'il ait été statué sur la demande d'aide. (...). Le débit du service d'accès à internet maintenu peut être restreint par l'opérateur, sous réserve de préserver un accès fonctionnel aux services de communication au public en ligne et aux services de courrier électronique⁴⁰³.

Placer le besoin d'accéder à Internet — et son cousin, l'accès au réseau téléphonique — presque sur le même plan que le besoin du foyer en eau ou en électricité constitue assurément un symbole fort. La même loi a entendu protéger par ailleurs un public présentant une autre forme de « fragilité » : celui des personnes handicapées⁴⁰⁴. Les sites Internet publics doivent être conçus pour leur être accessibles, sous peine de sanction administrative⁴⁰⁵.

120. Le principe d'une liberté de navigation – Le bloc de constitutionnalité et la loi ordinaire française protègent donc l'aptitude des citoyens à se connecter au réseau. Ce premier droit n'est qu'une coquille vide s'il n'est pas possible, ensuite, de profiter de cet accès pour communiquer, c'est-à-dire pour produire ou recevoir des informations. La liberté d'expression connaît des limites, qui seront bientôt examinées en détail. Qu'en est-il de la liberté de simplement prendre connaissance de contenus en ligne ? La consommation de médias traditionnels n'est pas réprimée,

403. - Art. L. 1165-3 du Code de l'action sociale et des familles, dans sa rédaction issue de la loi 2016-1321 précitée.

404. - C'est la loi n° 2016-1321 précitée qui opte pour cette présentation, en regroupant l'accès de base à Internet et l'accès des personnes handicapées aux sites Internet publics dans un chapitre intitulé « accès des publics fragiles au numérique » (art. 105 et s. de la loi).

405. - Art. 106 de la loi n° 2016-1321 précitée.

qu'il s'agisse d'allumer une radio et de la régler sur une certaine fréquence, ou de se rendre dans une librairie et d'y acheter n'importe quel écrit disponible sur ses rayonnages. En va-t-il de même en matière numérique, autrement dit : peut-on jouir sans crainte d'une liberté de navigation ?

La consultation du Code pénal, il y a peu, imposait une réponse négative. Un comportement était incriminé, qui consistait seulement à charger — à plusieurs reprises — un site dans la mémoire d'un navigateur afin d'en prendre connaissance :

Le fait de consulter habituellement un service de communication au public en ligne mettant à disposition des messages, images ou représentations soit provoquant directement à la commission d'actes de terrorisme, soit faisant l'apologie de ces actes lorsque, à cette fin, ce service comporte des images ou représentations montrant la commission de tels actes consistant en des atteintes volontaires à la vie est puni de deux ans d'emprisonnement et de 30 000 € d'amende.

Le présent article n'est pas applicable lorsque la consultation est effectuée de bonne foi, résulte de l'exercice normal d'une profession ayant pour objet d'informer le public, intervient dans le cadre de recherches scientifiques ou est réalisée afin de servir de preuve en justice⁴⁰⁶.

Le législateur avait sans doute conscience du risque d'inconstitutionnalité présenté par un texte réprimant le simple fait de s'exposer à des informations. Les deux alinéas le révèlent, chacun à sa manière. Le premier vise les propos encourageant à la commission d'actes de terrorisme ou faisant l'apologie du terrorisme, mais uniquement lorsqu'ils sont accompagnés d'images de tueries. Voilà qui instaure une curieuse hiérarchie dans l'horreur : il serait acceptable de consulter de tels propos non illustrés, mais l'inclusion d'une image dans la page Web en changerait profondément la nature. Le second alinéa reconnaît qu'il existe des motifs légitimes de consulter de tels discours de haine, mais adopte une curieuse démarche consistant à juxtaposer des cas précis — le journalisme, la recherche scientifique, la constitution de preuves vouées à être produites en justice — avec une exception à caractère général, au contenu totalement indéterminé : la « consultation de bonne foi ». On imagine que se connecter un site en ayant décidé par avance que son contenu était abject constituerait une telle consultation, l'internaute ne s'exposant au contenu que pour renforcer son sentiment d'horreur et rejeter les idées exposées avec plus de détermination encore. Cela poserait toutefois un problème pratique insurmontable, car ce serait à l'internaute de rapporter la preuve, quasiment impossible, d'un pur état psychologique. Cela poserait aussi et surtout un problème de fond : de tels contenus peuvent être consultés par des individus n'ayant pas *a priori* de position ni de sympathie, ni d'antipathie pour la propagande qui s'y trouve, voire par des individus qui les recherchaient en pensant y adhérer, mais qui éprouvent finalement un sentiment de rejet une fois

406. - Art. 421-2-5-2 du Code pénal, créé par une loi du 3 juin 2016 n° 2016-731 et aujourd'hui abrogé.

qu'ils y sont confrontés. Sont-ce des consultations « de bonne foi »? La pénalisation d'une consultation d'information apparaît en définitive au mieux inapplicable, au pire dangereuse.

Le Conseil constitutionnel ne s'y est pas trompé. Saisi d'une question prioritaire de constitutionnalité relative aux dispositions pénales précitées, il décide :

(...) au regard de l'exigence de nécessité de l'atteinte portée à la liberté de communication, les autorités administrative et judiciaire disposent, indépendamment de l'article contesté, de nombreuses prérogatives, non seulement pour contrôler les services de communication au public en ligne provoquant au terrorisme ou en faisant l'apologie et réprimer leurs auteurs, mais aussi pour surveiller une personne consultant ces services et pour l'interpeller et la sanctionner lorsque cette consultation s'accompagne d'un comportement révélant une intention terroriste, avant même que ce projet soit entré dans sa phase d'exécution.

En second lieu, s'agissant des exigences d'adaptation et de proportionnalité requises en matière d'atteinte à la liberté de communication, les dispositions contestées n'imposent pas que l'auteur de la consultation habituelle des services de communication au public en ligne concernés ait la volonté de commettre des actes terroristes ni même la preuve que cette consultation s'accompagne d'une manifestation de l'adhésion à l'idéologie exprimée sur ces services. Ces dispositions répriment donc d'une peine de deux ans d'emprisonnement le simple fait de consulter à plusieurs reprises un service de communication au public en ligne, quelle que soit l'intention de l'auteur de la consultation, dès lors que cette consultation ne résulte pas de l'exercice normal d'une profession ayant pour objet d'informer le public, qu'elle n'intervient pas dans le cadre de recherches scientifiques ou qu'elle n'est pas réalisée afin de servir de preuve en justice.

Si le législateur a exclu la pénalisation de la consultation effectuée de « bonne foi », les travaux parlementaires ne permettent pas de déterminer la portée que le législateur a entendu attribuer à cette exemption alors même que l'incrimination instituée, ainsi qu'il vient d'être rappelé, ne requiert pas que l'auteur des faits soit animé d'une intention terroriste. Dès lors, les dispositions contestées font peser une incertitude sur la licéité de la consultation de certains services de communication au public en ligne et, en conséquence, de l'usage d'Internet pour rechercher des informations.

Il résulte de tout ce qui précède que les dispositions contestées portent une atteinte à l'exercice de la liberté de communication qui n'est pas nécessaire, adaptée et proportionnée (...)⁴⁰⁷.

Quelques jours seulement après cette décision, le Parlement a choisi d'adopter un nouveau texte réprimant la consultation de sites terroristes. Afin de répondre aux critiques des Sages, il est cependant exigé que « (...) cette consultation s'accompagne d'une manifestation de l'adhésion à l'idéologie exprimée sur ce service »⁴⁰⁸. Cette modification change tout et le texte nouveau semble même assez inutile, puisqu'une manifestation positive d'adhésion à un discours d'apologie du

407. - Décision n° 2016-611 QPC du 10 février 2017, considérants 13 et suivants.

408. - Art. 421-2-5-2 du Code pénal, issu de l'art. 24 de la loi n° 2017-258 du 28 février 2017 relative à la sécurité publique.

terrorisme constitue par elle-même une infraction pénale⁴⁰⁹. Le simple fait de s'exposer à un contenu disponible en ligne n'est donc plus réprimé, et une liberté de navigation, appendice de la liberté de communication, semble ainsi reconnue aux internautes. Une exception existe cependant.

121. L'exception à la liberté de navigation – Depuis 2007, la loi pénale réprime le fait de « consulter habituellement ou en contrepartie d'un paiement un service de communication au public en ligne » mettant à disposition des images pédopornographiques⁴¹⁰. En effet, le premier alinéa du texte était insuffisant, qui dispose :

Le fait, en vue de sa diffusion, de fixer, d'enregistrer ou de transmettre l'image ou la représentation d'un mineur lorsque cette image ou cette représentation présente un caractère pornographique est puni de cinq ans d'emprisonnement et de 75 000 euros d'amende.

Une telle définition frappait les internautes ayant téléchargé des fichiers sur leur disque dur ou ayant réalisé des tirages papier, mais pas ceux qui se contentaient de les afficher dans leur navigateur⁴¹¹. Il parut nécessaire de réprimer spécifiquement la simple consultation de sites.

On comprend mieux, à présent, pourquoi le délit de consultation habituelle de sites terroristes reposait sur la présence d'images dans la page de propagande : le modèle constitué par le texte réprimant la visite de sites pédophiles a purement et simplement été repris. C'était une erreur. Comme le relève un avocat, « consulter un site pédopornographique est un acte en soi, un acte sexuel »⁴¹². C'est la raison pour laquelle aucune exception n'est prévue en matière d'images pédophiles, tandis que le législateur s'est perdu dans un entrelacs d'échappatoires générales et spéciales en matière terroriste : s'exposer à des images pédophiles est un acte univoque ; consulter une page de propagande, fût-elle particulièrement abjecte et accompagnée d'illustrations, est un acte équivoque.

122. Plan - La liberté de navigation connaît donc une exception bien réelle, mais dont les particularismes conduisent à penser qu'elle restera unique : il est interdit de s'exposer

409. - Art. 421-2-5 du Code pénal.

410. - Art. 227-23 al. 4 C. pén. Cet alinéa a été introduit par l'art. 35 de la loi n° 2007-297 du 5 mars 2007 relative à la prévention de la délinquance.

411. - Cass. crim., 5 janv. 2005, n° 04-82524 : « les juges retiennent que les images observées n'ont été ni imprimées ni enregistrées sur un support et que la simple consultation de sites pornographiques mettant en scène des mineurs ne suffit pas à caractériser le délit prévu par l'article 227-23, alinéa 4, du Code pénal ; Attendu qu'en prononçant ainsi, la cour d'appel a justifié sa décision ». Le pourvoi faisait valoir que la consultation du site entraînait le téléchargement automatique des images dans un fichier temporaire situé sur le disque dur, mais l'argument n'a pas été retenu (alors même que cette mémoire cache peut être à nouveau consultée ultérieurement par l'internaute sans qu'il soit besoin de retourner sur le site). Sur cette question, V. par ex. F. Chopin, « Cybercriminalité » in *Rép. pén. Dalloz*, n° 110.

412. - Maître Olivier Iteanu, président d'honneur de l'*Internet society*, cité dans P. Hérard, « Délit de consultation de sites Internet : une loi inapplicable ? », article du 18/07/16 sur information.tv5monde.com.

volontairement à des images pédopornographiques. La catégorie des contenus profondément contraires à nos valeurs sociales est certes bien plus vaste, mais le seul fait d'en prendre connaissance ne peut faire l'objet d'une répression pénale. L'encadrement des communications numériques se concentre non pas sur les consommateurs d'information, mais sur deux autres catégories d'acteurs. La première, évidente, est constituée des personnes exprimant des opinions, produisant des contenus et de l'information (section 1). La seconde, plus discrète, mais au moins aussi importante, est constituée des intermédiaires, des plateformes qui manipulent, trient, classent, présentent, hiérarchisent l'information, autrement dit : qui contribuent à la rendre visible – ou invisible (section 2).

Section 1 – La production de l'information

123. De la pluralité à la multitude – L'article 11 de la Déclaration des Droits de l'Homme de 1789 a été évoqué plus haut, sans que son contenu soit reproduit. Il est temps d'en rappeler les termes : « La libre communication des pensées et des opinions est un des droits les plus précieux de l'Homme : tout Citoyen peut donc parler, écrire, imprimer librement, sauf à répondre de l'abus de cette liberté dans les cas déterminés par la Loi ». Commentant ce texte, Mirabeau déclarait :

On vous laisse une écriture pour écrire une lettre calomnieuse, une presse pour un libelle, il faut que vous soyez punis quand le délit est consommé. Or ceci est répression et non restriction. C'est le délit que l'on punit, et l'on ne doit pas gêner la liberté des hommes sous prétexte qu'ils veulent commettre des délits⁴¹³.

Il se prononçait ainsi contre les mesures de censure et d'autorisation préalable. Un siècle plus tard, la loi de 1881 est exactement en ce sens, qui adopte un régime dit « répressif » : les atteintes à la liberté d'expression ne sont pas empêchées, mais punies une fois qu'elles ont été commises⁴¹⁴. Du moins est-ce le principe, auquel il est porté atteinte en de rares et graves occasions, pour des durées limitées, par le juge judiciaire des référés⁴¹⁵. Récemment, des spectacles ont également été interdits à titre préventif par le juge administratif des référés, en tant qu'ils créaient un risque de trouble à

413. - Cité par F. Pillet et T. Mohamed Soilihi, *L'équilibre de la loi du 29 juillet 1881 à l'épreuve d'Internet. Rapport d'information fait au nom de la commission des lois*, n° 767, consultable sur senat.fr.

414. - Loi du 29 juillet 1881 sur la liberté de la presse. Ailleurs en Europe, l'interdiction de la censure est souvent consacrée directement et explicitement par la Constitution : B. Beigner, B. de Lamy et E. Dreyer (ss. la dir.), *Traité de droit de la presse et des médias*, Litec, 2009, n° 116.

415. - B. Beigner, B. de Lamy et E. Dreyer, *op. cit.*, n° 118. La Cour européenne des Droits de l'Homme a admis que le juge des référés pouvait prendre des mesures d'interdiction de diffusion d'un ouvrage, lorsque des motifs « pertinents et suffisants » étaient mis en évidence et que la mesure avait un caractère temporaire. Dans cette affaire, l'interdiction de publication de l'ouvrage *Le Grand secret*, relatif à la santé du président Mitterrand, était justifiée dans un premier temps, mais avait été prolongée à l'excès (CEDH, *Editions Plon c./ France*, 18 mai 2004, n° 58148/00).

l'ordre public⁴¹⁶. Quittons l'exception pour revenir à la règle : chacun est libre d'exprimer publiquement des pensées et opinions. Avant l'apparition d'Internet, de nombreuses publications papier et autres émissions radiophoniques petites et minuscules avaient déjà pris place au côté des « grands médias ». La liberté de « la presse » vivait aussi bien au travers d'une « feuille de chou » animée par trois lycéens qu'à travers *Le Monde*, *Libération* ou *le Figaro*. Mais une fois ramené à l'ensemble de la population, le modèle était bien celui d'un petit nombre de tribuns s'adressant à une foule de lecteurs et d'auditeurs passifs : des pyramides. Depuis le développement du Web, des forums de discussion et surtout des réseaux sociaux, chacun ou presque fait usage de la liberté consacrée à l'article 11 de la Déclaration des Droits de l'Homme. « Tout Citoyen peut » écrire et publier librement est devenu « Tout Citoyen écrit et publie ». La pyramide est devenue ruche, une « conversation mondiale sans fin »⁴¹⁷.

124. **Plan** – Si le défi lancé au droit de la presse n'était que quantitatif, il serait déjà considérable. Il est facile d'identifier et de sanctionner les propos excessifs lorsqu'ils émanent d'un petit nombre de citoyens actifs. Plus le nombre d'acteurs à réguler augmente, plus l'ineffectivité du droit menace. Mais l'influence du numérique ne se limite pas à précipiter une cascade d'informations sur un système juridique et judiciaire menacé d'écroulement. Des spécificités techniques amènent, sinon à poser des questions entièrement nouvelles, du moins à donner une importance de premier plan à des problèmes jusqu'ici marginaux⁴¹⁸. Les difficultés sont de deux ordres : certaines concernent la détermination même de ce qu'est une expression illicite (I), tandis que d'autres affectent la capacité à sanctionner des propos dont le caractère excessif est bel et bien établi (II).

I – Les difficultés tenant à la détermination de l'expression illicite

125. **Plan** – Au nombre de ces difficultés qui, sans être entièrement inédites, sont largement aggravées par l'usage des technologies numériques, il faut compter la simple reproduction des

416. - Conseil d'État, ordonnance du 9 janvier 2014, *Société Les Productions de la Plume et M. D.*, requête numéro 374508. Le juge relève notamment que : « ce spectacle, tel qu'il est conçu, contient des propos de caractère antisémite, qui incitent à la haine raciale, et font, en méconnaissance de la dignité de la personne humaine, l'apologie des discriminations, persécutions et exterminations perpétrées au cours de la Seconde Guerre mondiale ». La référence à la dignité humaine comme composante de l'ordre public évoque évidemment le célèbre arrêt sur le lancer de nains du Conseil d'État, Assemblée, 27 octobre 1995, *Commune de Morsang-sur-Orge*, requête numéro 136727, publié au recueil. Mais dans cette décision antérieure, ce n'est pas une forme d'expression qui avait été interdite — sauf à adopter de cette notion une vision particulièrement extensive — mais une réification du corps humain. Dans le même sens : TA Paris, ord. du 9 déc. 2014, n° 1430123/9 : *ADJA*, 2015, p. 199.

417. - Sur cette expression, V.supra, n°118.

418. - Les développements à suivre seront largement nourris par notre recherche antérieure : « La liberté d'expression sur les réseaux sociaux en droit français », in *Droit et réseaux sociaux*, dir. V. Ndiou, coll. LEJEP, Lextenso, 2015, p. 39.

propos illicites d'autrui. En effet, une spécificité majeure du numérique est de permettre la réalisation de copies instantanées et quasiment gratuites d'informations. Or, les outils de communication numérique, en particulier les réseaux sociaux, emploient massivement cette possibilité technique en permettant à leurs utilisateurs de répercuter des propos tenus par un tiers à leurs propres « amis » ou « abonnés », qui n'en étaient pas initialement destinataires. Celui qui « partage », qui « retweete », qui « copie et colle » les propos d'autrui n'entend pas nécessairement les assumer ni même y adhérer, mais participe à leur diffusion. Il nous faudra séparer cette délicate question de l'expression « relayée » (B) des difficultés suscitées par l'expression véritablement personnelle (A).

A – L'expression personnelle

126. Le numérique, simple support d'expression – Peut-on imaginer des propos qu'il serait licite de formuler partout ailleurs que sur Internet, mais dont la publication en ligne serait contraire à la loi ? Une récente loi semble accréditer cette idée, que la rapporteure à l'Assemblée nationale — largement suivie par les médias — qualifiait de « délit d'entrave numérique » à l'interruption volontaire de grossesse⁴¹⁹. Le délit d'entrave à l'IVG date de 1993 et a été modifié à plusieurs reprises, pour sanctionner les personnes empêchant l'exercice du droit à l'interruption volontaire de grossesse, en usant de pressions physiques ou morales⁴²⁰. Une nouvelle extension a été proposée, l'exposé des motifs de la proposition de loi ne faisant pas mystère de ce qu'il visait principalement des auteurs des propos en ligne.

(...) la tentative d'entrave prend de nouvelles formes sur Internet. Une opinion explicitement exprimée relève des principes de liberté d'expression et d'opinion qu'il ne s'agit pas de remettre en cause. En revanche, induire délibérément en erreur, intimider et/ou exercer des pressions psychologiques ou morales afin de dissuader de recourir à l'IVG, comme le font certains sites Internet, se situe sur un tout autre terrain.

Comme le montre le rapport sur l'accès à l'IVG du Haut Conseil à l'égalité (HCE) entre les femmes et les hommes rendu en novembre 2013, on observe depuis quelques années une montée en puissance très importante de sites cherchant à tromper délibérément les internautes en se faisant passer, au premier abord, pour des sites « purement informatifs »⁴²¹.

Le Code de la santé publique a donc été modifié, de sorte que l'on réprime aujourd'hui « (...) le fait d'empêcher ou de tenter d'empêcher de pratiquer ou de s'informer sur une interruption

419. - V. par ex. le compte-rendu des travaux de la commission mixte paritaire sur cette loi n° 2017-347 du 20 mars 2017 relative à l'extension du délit d'entrave à l'interruption volontaire de grossesse. Mme Coutelle utilise à plusieurs reprises le nom de « délit d'entrave numérique ».

420. - Le texte d'origine a été institué par la loi n° 93-121 du 27 janvier 1993.

421. - Extrait de l'exposé des motifs de la loi précitée 2017-347.

volontaire de grossesse (...) **par tout moyen, y compris par voie électronique ou en ligne**, notamment par la diffusion ou la transmission d'allégations ou d'indications de nature à induire intentionnellement en erreur [...] »⁴²². La lecture du texte révèle que, d'un point de vue rigoureusement juridique, la communication en ligne constitue un simple exemple de moyen susceptible d'être employé. Le fait qu'il soit en pratique le plus courant n'y change rien : la diffusion de tracts sur papier pourrait pareillement provoquer les foudres du droit pénal. D'ailleurs, le Sénat avait adopté une version du texte s'en tenant à l'expression « par tout moyen »⁴²³. La rapporteure pour la commission des affaires sociales de la Haute assemblée avait expliqué : « Cette rédaction permet d'écarter toute ambiguïté sur le fait que la communication par voie électronique fait bien partie intégrante des moyens par lesquels peuvent s'exercer des pressions psychologiques ou morales »⁴²⁴. En commission mixte paritaire, la rapporteure de l'Assemblée nationale s'en était indignée :

(...) le texte adopté par le Sénat gomme toute référence explicite au délit d'entrave « numérique », qui est l'objet initial et fondamental de la proposition de loi, autrement dit, sa raison d'être : c'est pourquoi le fait de supprimer toute référence aux moyens électroniques et numériques ne me semble pas acceptable.

*En tant que rapporteure pour l'Assemblée nationale, je tiens donc particulièrement au maintien des précisions apportées par notre assemblée [...] sur la caractérisation du support, numérique et électronique, afin de bien caractériser ce délit d'entrave numérique*⁴²⁵.

L'aveu est clair : la mise en exergue du numérique au sein du texte constitue pour certains parlementaires un moyen d'afficher leur volontarisme politique. Elle est inutile juridiquement, car décidément non, on n'imagine guère de propos qu'il soit licite de prononcer publiquement, ou de publier sur un tableau d'affichage, mais qu'il soit punissable de formuler en ligne.

127. Le numérique, support particulier d'expression – S'il est donc clair que le caractère numérique du support ne peut être *directement* un critère décisif en matière de qualification juridique, il faut en revanche concéder qu'il est plus propice, de fait, à certaines modalités d'expression qui posent des problèmes de droit. En raison de ses caractéristiques techniques, le support numérique provoque *indirectement* des difficultés récurrentes. Ainsi, il est fréquent que les internautes se réfugient derrière le caractère anonyme (1) ou privé (2) de leurs propos pour contester

422. - Art. L. 2223-2 al. 1 du Code de la santé publique. Souligné par nous.

423. - Texte adopté par le Sénat le 7 décembre 2016.

424. - Rapport n° 183 (2016-2017) de Mme Stéphanie Riocreux, fait au nom de la commission des affaires sociales, déposé le 6 décembre 2016.

425. - Compte-rendu précité des travaux de la commission mixte paritaire.

avoir commis une faute. Ces problèmes, répétons-le, ne sont certes pas nouveaux dans leur principe, mais se posent en ligne à une fréquence et avec une intensité particulières.

1. - Le caractère anonyme du propos

128. L'impact de l'anonymat sur la licéité de l'expression - L'anonymat ou le pseudonymat n'ont pas attendu le numérique pour exister. Depuis qu'il existe des artistes, des opposants politiques, des maîtres chanteurs et des délateurs, celui qui s'exprime peut chercher à jeter un voile sur son identité, pour les raisons les plus nobles ou pour les plus viles. Mais Internet, pour des raisons techniques déjà longuement analysées, est un espace entièrement anonyme *ab initio*⁴²⁶. Il était donc prévisible que des rencontres entre anonymat et liberté d'expression s'y produisent en nombre. Mais il ne sera pas traité, ici, de l'anonymat comme simple obstacle à la sanction d'un propos dont l'illicéité ne fait aucun doute⁴²⁷. La question sera celle de savoir si l'anonymat ou le pseudonymat est susceptible de faire rentrer à l'intérieur des limites de la liberté d'expression des propos qui, s'ils avaient contenu de véritables identités, auraient été constitutifs d'une faute civile, disciplinaire ou pénale. Dans les exemples ci-après développés, nous constaterons que l'anonymat masque parfois l'identité de l'auteur des propos, parfois l'identité de leur cible, parfois encore les deux à la fois.

129. L'anonymat évitant la commission d'une faute - Une première hypothèse concerne les professionnels souhaitant relater publiquement certaines de leurs activités, sans pour autant violer le secret auquel la loi les astreint. Le Code pénal dispose en effet :

*La révélation d'une information à caractère secret par une personne qui en est dépositaire soit par état ou par profession, soit en raison d'une fonction ou d'une mission temporaire, est punie d'un an d'emprisonnement et de 15 000 euros d'amende*⁴²⁸.

Nombreux sont les avocats ou les médecins, par exemple, qui tiennent un blog ou qui décrivent un cas auquel ils sont confrontés sur les réseaux sociaux. En masquant leur identité et celle de leurs clients ou patients, ils transforment le secret qu'ils ne sauraient trahir en une histoire abstraite qui ne porte préjudice à personne⁴²⁹.

426. - V.supra, n° 35 et s.

427. - Sur cette question, V.infra, n°153.

428. - Art. 226-13 C. pén.

429. - Parmi de nombreux exemples, citons les blogs des avocats Maître Eolas (www.maitre-eolas.fr) ou Maître Mo (maitremo.fr) ou le médecin Jaddo (www.jaddo.fr), qui prolongent leur journal en ligne sur des comptes Twitter.

Une seconde hypothèse concerne des propos présentant la nature non pas de simple récit destiné à édifier les lecteurs, mais plutôt de mises en cause, d'attaques, d'agressions. Elles pourraient être qualifiées d'injures ou de diffamations si elles étaient dirigées contre des cibles identifiées, mais constituent un simple exutoire sans conséquence juridique lorsqu'elles visent des abstractions. Ainsi une salariée, fort mécontente de la manière dont elle était traitée par la société qui l'employait, avait-elle choisi le pseudonyme « Petite anglaise » pour exposer régulièrement sur un blog, aux yeux de tous, les motifs de son courroux. Pour autant, elle ne révélait jamais ni son véritable nom, ni celui de son entreprise. Elle fut pourtant licenciée lorsque sa hiérarchie découvrit l'existence du site. Le Conseil des prud'hommes jugea ce licenciement dépourvu de cause réelle et sérieuse, relevant :

[...] que le blog était écrit en anglais et que Madame Petite ANGLAISE s'identifiait sur le blog sous le pseudonyme «la petite anglaise» et qu'il n'apparaît à aucun moment le nom du le CABINET DIXON WILSON ni les noms d'aucun salarié que le CABINET DIXON WILSON n'a jamais été visé, ni identifié pendant les deux années de vie du blog avant le licenciement de Madame Petite ANGLAISE (...) Que le Conseil n'a constaté aucun propos diffamatoire ou injure qui porte atteinte à l'entreprise, car il n'y a aucun moyen de pouvoir identifier les personnes ; que le Conseil affirme que Madame Petite ANGLAISE n'a fait que relater, sous une certaine forme de romance, sa vie personnelle et parfois professionnelle tout en restant inidentifiable[...]⁴³⁰.

De la même façon, la Cour d'appel de Reims annula une sanction disciplinaire prononcée contre un salarié ayant laissé libre cours à son courroux sur sa page Facebook, sans pour autant nommer personne⁴³¹. Encore faut-il qu'il ne soit pas trop simple, pour les lecteurs, de reconnaître les individus visés par des éléments de contexte aisément déchiffrables : attention si le masque glisse et tombe à terre⁴³². C'est qu'il n'existe pas uniquement des situations d'anonymat pur ou d'identité dévoilée : des nuances peuvent s'insinuer entre ces deux extrêmes.

130. Les degrés dans l'anonymat - Un employé d'une chaîne de restauration rapide avait créé un compte Twitter intitulé @EquipierQuick. Il s'épanchait auprès de ses abonnés sur ses conditions de travail, décrites comme particulièrement rudes, et y ajoutait de violentes critiques concernant les manquements aux règles d'hygiène dans la préparation des repas. Voilà qui était de nature à dissuader la clientèle de se rendre dans les restaurants de la chaîne. Sans doute n'avait-il jamais désigné l'établissement franchisé précis pour lequel il travaillait, qu'il appelait dans ses messages

430. - Ces extraits d'une décision rendue durant l'été 2007 sont reproduits par le blogueur précité Maître Eolas sur son blog : <http://www.maitre-eolas.fr/post/2007/07/05/660-le-jugement-dans-l-affaire-petite-anglaise>.

431. - CA Reims, 9 juin 2010, n° 09/03205.

432. - Dans la décision précitée, la Cour estime que tel n'était pas le cas : « “(...) il apparaît clairement que dans le message, aucun nom n'a été indiqué par Monsieur C. et que le terme ‘chef’ ne s'apparente pas systématiquement à la relation professionnelle ; que l'employeur lui même hésite entre un collègue ou un membre de la direction ; qu'il existe en tout état de cause une ambiguïté sur la personne visée”.

« le Quick mystère ». Mais la réputation de la franchise elle-même, et indirectement celle de tous les franchisés, était évidemment atteinte. L'anonymat adopté était insuffisant. À l'instar d'une « Petite anglaise » qui se noyait dans l'océan grisâtre des travailleurs de bureau, « EquipierQuick » aurait été mieux inspiré de se fondre dans la fourmilière des employés du secteur de la restauration rapide, sans jamais révéler de quelle chaîne il était question. Cet anonymat, sans effet sur la qualification des propos, était, au mieux, un obstacle provisoire à la sanction, qu'il est toujours possible de surmonter. L'homme fut finalement licencié, et mis en examen pour diffamation⁴³³.

131. L'anonymat impuissant à éviter la faute - Dans l'affaire précédente, l'anonymat était insuffisamment et maladroitement employé. Mais il est des hypothèses dans lesquelles il semble purement et simplement inefficace, quelle que soit la manière dont il est mis en œuvre. Ainsi, deux magistrats — l'un juge du siège, l'autre membre du parquet — avaient créé des comptes Twitter sous les pseudonymes @BipdEd et @Proc_Gascogne. Ils s'y exprimaient séparément ou de concert, et leurs lecteurs savaient qu'ils appartenaient tous deux à la même juridiction. Au cours d'une audience correctionnelle à laquelle l'un siégeait comme assesseur, l'autre comme représentant du ministère public, ils échangèrent des messages moquant d'autres acteurs du procès : « *ça y est, j'ai fait pleurer le témoin* », ou encore « *un assesseur exaspéré qui étrangle sa présidente en pleine audience, ça vaut combien ?* ». Rien ne permettait, à la seule lecture des messages, de savoir quelle était la juridiction concernée, et moins encore de quelle affaire il s'agissait. Mais quelque temps plus tard, un journaliste mena l'enquête, perça à jour l'identité des deux hommes, et la révéla publiquement. Il devint possible d'en déduire durant quelle affaire les deux internautes avaient affiché une connivence qui n'a normalement pas sa place entre un juge indépendant et une partie au procès, ainsi qu'une tendance à ne pas prêter suffisamment d'attention au déroulement de l'audience. Le parquet crut nécessaire de faire appel, afin que l'affaire soit à nouveau jugée et que les critiques portant sur la décision de premier degré soient ainsi purgées.

Les messages échangés à la vue de tous se prêtent à deux analyses concurrentes. La première voudrait que le trouble soit né au moment où le pseudonymat a été brisé. Mais dans la mesure où il l'a été par un tiers, peut-on faire ce reproche aux deux hommes ? Il faudrait pour cela postuler que toute personne s'exprimant sous un faux nom pourrait un jour être démasquée, et qu'il faudrait pour cela fictivement la traiter comme si elle avait toujours révélé son identité. Les moyens illégaux, mais aussi légaux permettant de tracer les individus sont aujourd'hui tels que cela reviendrait à interdire l'expression pseudonyme, y compris par exemple aux avocats ou médecins blogueurs précédemment cités. Mais la deuxième analyse de cette affaire est plus radicale encore. Elle se

433. - M. Ferhallad, « L'ex équipier Quick mis en examen pour diffamation », article du 11/01/14, *laprovence.com*. Nous n'avons pas trouvé trace du dénouement de l'histoire.

découvre sous la plume du Conseil supérieur de la magistrature, qui rendit une décision disciplinaire contre le parquetier, comprenant le motif suivant : « [...] *le prétendu anonymat qu'apporteraient certains réseaux sociaux ne saurait affranchir le magistrat des devoirs de son état, en particulier de son obligation de réserve, gage pour les justiciables de son impartialité et de sa neutralité notamment durant le déroulement du procès* »⁴³⁴. Qu'un juge du siège et un représentant du parquet affichent leur connivence, et semblent peu attentifs au déroulement de l'audience a « (...) *porté atteinte à la confiance que les justiciables doivent pouvoir accorder aux décisions de justice* »⁴³⁵. Le raisonnement, parfaitement convaincant, est évidemment transposable hors de la magistrature. Il peut arriver qu'une personne, par ses propos ou publications, déshonore le corps ou la profession auquel il appartient, sans que la révélation ou le secret de son identité y change rien. Peu importe alors dans quelle juridiction, dans quelle étude ou dans quel cabinet, dans quel dossier et avec quel client ou patient les faits se sont produits. L'anonymat, procuré par Internet ou conquis d'une autre façon, n'est alors d'aucun secours.

Dans cette affaire, en revanche, le caractère public de l'expression a joué un rôle fondamental. Quand peut-on considérer que des propos publiés en ligne n'ont été adressés qu'à un cercle restreint et privé ?

2 - Le caractère privé du propos

132. Des outils de communication numérique à intimité variable - Qualifier une expression en ligne de publique ou de privée est une opération lourde d'enjeux. Quelques exemples en seront développés ci-après, qui montrent que l'intimité du propos peut s'opposer à ce qu'une faute soit retenue : dénigrer son employeur devant quelques amis choisis n'est pas justiciable d'une sanction disciplinaire ; tenir le même discours publiquement est une faute pouvant conduire au licenciement. Parfois, le cantonnement du propos à un cercle de destinataires précis ne suffira pas à dissiper son caractère fautif, mais modifiera l'incrimination pénale applicable et, partant, la peine encourue : tel est le cas en matière d'injures.

Internet est-il alors un espace public ou privé ? Il est impossible de répondre à cette question. Dire de quelqu'un qu'il s'exprime « sur Internet » n'est qu'une facilité de langage, qui ne correspond à aucune réalité technique. Internet n'est qu'un mode de transport d'informations, qui peut être mis au service d'outils de communication d'une très grande variété. Un site peut être accessible à tous ; l'accès à tout ou partie de son contenu peut à l'inverse être restreint à des

434. - <http://www.conseil-superieur-magistrature.fr>, rubrique « discipline des magistrats », décision P079.

435. - *Ibid.*

utilisateurs inscrits, dont le nombre et l'homogénéité ne peuvent être postulés par avance. S'agissant des réseaux sociaux, certains, comme Twitter, ont une vocation publique par défaut — les messages qui y sont rédigés peuvent être lus par n'importe qui, et sont indexés par des moteurs de recherche — mais les utilisateurs peuvent opter s'ils le souhaitent pour des « comptes protégés », chaque lecteur intéressé devant être au préalable adoubé par le titulaire du compte. Enfin, Twitter propose d'échanger ponctuellement des « messages privés » qui seront visibles uniquement par les destinataires : une personne, ou des dizaines, qui peuvent se connaître ou non. Facebook ou Google + peuvent être réglés plus finement encore. Entre les publications ouvertement publiques — par exemple, la « page » d'une société commerciale ou d'une association — et les messages privés, les messages peuvent être réglés très finement pour être consultables par un ou plusieurs « cercles d'amis » composés selon la volonté de l'utilisateur, ou par tous ses « amis », voire par « les amis de ses amis »⁴³⁶.

133. Importance des réglages et charge de la preuve — Deux cours d'appel ont eu à statuer — le même jour - sur le statut public ou privé d'un message posté sur Facebook, le plus fameux de ces réseaux sociaux. Les deux analyses divergent, tant du point de vue de la qualification que du régime juridique à appliquer. La Cour d'appel de Besançon, tout d'abord, écrit que :

*« [...] le réseau Facebook a pour objectif affiché de créer entre ses différents membres un maillage relationnel destiné à s'accroître de façon exponentielle par application du principe "les contacts de mes contacts deviennent mes contacts" et ce, afin de leur permettre de partager toutes sortes d'informations ; que ces échanges s'effectuent librement via "le mur" de chacun des membres auquel tout un chacun peut accéder si son titulaire n'a pas apporté de restrictions ; **qu'il s'en suit que ce réseau doit être nécessairement considéré, au regard de sa finalité et de son organisation, comme un espace public** ; qu'il appartient en conséquence à celui qui souhaite conserver la confidentialité de ses propos tenus sur Facebook, soit d'adopter les fonctionnalités idoines offertes par ce site, soit de s'assurer préalablement auprès de son interlocuteur qu'il a limité l'accès à son "mur" »⁴³⁷.*

436. - Le terme « ami », généralisé par Facebook, doit être considéré avec beaucoup de prudence, et signifie simplement qu'une personne B est présente au sein des contacts d'une personne A. Par le jeu des réglages qui viennent d'être décrits, il est tout à fait possible d'empêcher ce contact d'avoir connaissance des publications véritablement personnelles. Une cour d'appel a donc pu décider que : « le terme d'"ami" employé pour désigner les personnes qui acceptent d'entrer en contact par les réseaux sociaux ne renvoie pas à des relations d'amitié au sens traditionnel du terme et que l'existence de contacts entre ces différentes personnes par l'intermédiaire de ces réseaux ne suffit pas à caractériser une partialité particulière, le réseau social étant simplement un moyen de communication spécifique entre des personnes qui partagent les mêmes centres d'intérêt, et en l'espèce la même profession » (raisonnement repris, mais présenté comme l'exercice d'un pouvoir souverain d'appréciation par Cass., 2e civ., 5 janv. 2017, n° 16-12.394). Un avocat tentait de récuser un membre de la formation de jugement du conseil de l'ordre, appelé à statuer dans une instance disciplinaire contre lui, en raison de ses amitiés sur Facebook.

437. - CA Besançon, 15 nov. 2011, n° 10/02642 : CCE, 2012, n° 4, 2012, p. 37, obs. A. Caprioli. Souligné par nous.

La motivation n'est pas limpide, qui considère tout à la fois que ce réseau est par nature « un espace public », et qu'il faut tenir compte des réglages adoptés par l'utilisateur. Toute la question est alors de savoir qui doit apporter la preuve que le compte était configuré de manière à assurer la confidentialité des propos. En relevant que les réglages par défaut de la plateforme donnent une publicité maximale aux messages qui s'y trouvent, et en ajoutant qu'il appartient à l'utilisateur de prendre des initiatives en sens contraire s'il le souhaite, la Cour d'appel de Besançon semble faire peser la charge de la preuve sur l'auteur des propos, non sur leur cible. L'arrêt de la Cour d'appel de Rouen n'est pas en ce sens, dans lequel on peut lire :

[...] il ne peut être affirmé de manière absolue que la jurisprudence actuelle nie à Facebook le caractère d'espace privé, alors que ce réseau peut constituer soit un espace privé, soit un espace public, en fonction des paramétrages effectués par son utilisateur. À cet égard, aucun élément ne permet de dire que le compte FACEBOOK tel que paramétré par Mlle R. ou par les autres personnes ayant participé aux échanges autorisait le partage avec les amis de ses amis ou toute autre forme de partage à des personnes indéterminées, de nature à faire perdre aux échanges litigieux leur caractère de correspondance privée⁴³⁸.

Refusant quant à elle de qualifier Facebook « d'espace public » par nature, la juridiction rouennaise rejoint son homologue bisontine sur l'importance des choix effectués par l'utilisateur lorsqu'il paramètre son compte. Mais elle reprend ses distances avec l'arrêt précédent lorsqu'elle aborde la charge de la preuve. En relevant qu'aucun élément ne lui était présenté accréditant la perte de confidentialité des propos, elle fait peser ce fardeau sur la cible des messages et non sur leur auteur. Deux arguments militent en faveur de cette solution : l'un d'ordre théorique, l'autre d'ordre pratique. Le premier consiste à dire qu'en matière répressive — que l'enjeu soit une sanction disciplinaire ou pénale -, il n'appartient pas à la personne mise en cause de faire la démonstration de son innocence. Le second argument repose sur la quasi-impossibilité, pour l'auteur des propos, d'apporter la démonstration de ce qu'étaient les paramètres de son compte à un instant donné. Dans la mesure où ces réglages peuvent être modifiés à chaque instant, leur état au moment du litige — des semaines ou des mois après la publication — sera sans valeur. Or, l'auteur des propos n'aura pas pris la peine de se ménager une preuve des réglages à l'époque où il aura posté son message, car on imagine qu'il n'a pas nécessairement anticipé le contentieux qui s'ensuivrait. En revanche, lorsque la victime découvre la publication qui la vise, il lui est facile de faire constater par huissier, par exemple, que les propos concernés s'affichent dans son propre fil d'actualités, ou sur celui d'un collègue de l'auteur.

438. - CA Rouen, 15 nov. 2011, n° 11/01827 : CCE, 2012, n° 9, p. 42, obs. E. Caprioli. Nous soulignons.

134. Le critère de la communauté d'intérêts - La Cour de cassation a eu à connaître d'une affaire d'injures proférées sur les réseaux sociaux. Là encore, la question était de savoir si les propos avaient un caractère public ou privé. Dans les deux cas, toutefois, le comportement est punissable, mais l'infraction d'injures publiques est plus grave et plus sévèrement réprimée : là était l'enjeu⁴³⁹. Le raisonnement tenu par la cour d'appel et approuvé par la Haute juridiction est le suivant : « après avoir constaté que les propos litigieux avaient été diffusés sur les comptes ouverts par Mme X... tant sur le site Facebook que sur le site MSN, lesquels n'étaient en l'espèce accessibles qu'aux seules personnes agréées par l'intéressée, en nombre très restreint, la cour d'appel a retenu, par un motif adopté exempt de caractère hypothétique, que celles-ci formaient **une communauté d'intérêts** »⁴⁴⁰.

Le critère ici mobilisé de la « communauté d'intérêts » est connu depuis longtemps en matière de communications non électroniques, et son transport dans le monde numérique ne suscite aucune objection de principe⁴⁴¹. Entre les deux extrêmes que constituent la page totalement publique d'une part, et la conversation confidentielle avec un unique interlocuteur d'autre part, une large gamme de situations peut se rencontrer. Le critère de la « communauté d'intérêts » en offre une grille de lecture. Encore faut-il s'entendre sur sa signification. On considère classiquement que le juge doit rechercher, chez les destinataires du message, une « appartenance commune, des aspirations ou des objectifs partagés »⁴⁴². Autrement dit, une communauté d'intérêts se reconnaît à l'homogénéité de sa composition, ce qui n'exclut pas qu'elle compte des membres assez nombreux. C'est ainsi qu'il a été jugé qu'une note adressée à l'ensemble du personnel d'une entreprise était cantonnée à une communauté d'intérêts⁴⁴³. Tout au contraire, un courrier électronique ayant été adressé à la fois aux membres d'un syndicat et aux membres d'une formation politique, une cour d'appel a considéré que : « (...) si les destinataires du courrier électronique incriminé peuvent avoir des intérêts communs, ils font partie de groupements qui constituent des entités distinctes, ne partageant pas nécessairement les mêmes objectifs et ayant des domaines d'action différents »⁴⁴⁴. Seule comptait la

439. - Les injures publiques sont punies d'une amende de 12000 euros (art. 33 al. 2 de la loi du 29 juillet 1881 sur la liberté de la presse). Les injures non publiques sont punies de l'amende prévue pour les contraventions de 1ère classe (art. R. 621-2 C. pén.).

440. - Cass. 1ère civ., 10 avr. 2013, n° 11-19530 : Bull. civ., I, n° 70 ; JCP G, n° 17, p. 816, obs. L. Marino ; RLDI, 2013, n° 93, p. 47, obs. J. de Romanet et L. Costes ; Légipresse, 2013, n° 305, p. 270 ; JCP S, 2013, n° 23, p. 18, obs. B. Bossu ; Gaz. Pal., 19 juin 2013, n° 170, p. 14, obs. P. Piot. *Adde* A. Lepage, « La notion de communauté d'intérêts à l'épreuve des réseaux sociaux », *CCE*, 2013, n° 7, p. 43. Souligné par nous.

441. - A. Lepage, « La notion de communauté... », art. préc.

442. - Y. Mayaud, *Rev. sc. crim.* 1998, p. 104, obs. sur Cass. crim., 3 juin 1997 : Bull. crim. 1997, n° 218, cité par A. Lepage, art. préc.

443. - Cass. 1ère civ., 31 janv. 2008, n° 07-12643 : Bull. civ., I, n° 33.

444. - Cass. crim., 28 avr. 2009, n° 08-85.249, inédit.

cohérence, et le nombre des destinataires restait hors de la discussion. Aussi un commentateur s'est-il étonné des motifs de l'arrêt relatif à Facebook et MSN, centrés sur le « nombre restreint » de contacts⁴⁴⁵. Reconnaissons que, de fait, le faible nombre de destinataires d'un message augmente les chances qu'une seule communauté d'intérêts ait été touchée ; mais là n'est pas le critère, en droit. Il n'y a pas de raison évidente pour laquelle la notion de « communauté d'intérêts » s'émanciperait, en droit des réseaux sociaux, de la manière dont elle a été appliquée par le passé aussi bien aux communications non électroniques qu'aux emails. Or, si certains réseaux sociaux spécialisés, par exemple à usage strictement professionnel, présentent une certaine homogénéité dans les contacts accumulés par l'internaute, ce n'est généralement pas le cas des réseaux généralistes comme Facebook. Quel utilisateur de cette plateforme peut dire que sa liste « d'amis » forme une communauté d'intérêts, au sens qui vient d'être décrit ? Y faire cohabiter un collègue de bureau et un camarade de collège, c'est déjà briser potentiellement la communauté - sauf à considérer que deux personnes ayant un ami commun partagent des « aspirations communes », ce qui ferait exploser la notion. Cela s'explique fort bien : lorsqu'un courrier postal ou même électronique est envoyé, une liste de destinataires est constituée spécialement pour l'occasion, tandis que les publications sur un réseau social généraliste sont, par défaut, dirigées vers une foule bigarrée d'amis véritables, de vagues connaissances et de collègues. Il appartient à l'utilisateur de ces outils, lorsqu'il rédige une publication sensible, de prendre le temps d'en restreindre la visibilité au strict nécessaire.

Le critère de la communauté d'intérêts n'est pas resté cantonné aux affaires mettant en œuvre la loi de 1881 sur la liberté de la presse. Dans un litige de droit du travail, la Cour d'appel de Versailles a pu juger que : « S'agissant de la possibilité pour l'employeur de se fonder sur les propos tenus par la salarié sur son espace facebook, il ne peut être soutenu qu'il s'agit d'un espace public dès lors qu'il n'est pas discuté qu'il était paramétré pour être limité aux « amis » de Mme Le G. **qui formaient une communauté d'intérêts** et qu'il n'était donc accessible qu'aux seules personnes, en nombre restreint, agréées par la salariée »⁴⁴⁶.

En revanche, toujours en matière de licenciement disciplinaire, la Cour de cassation a rendu un arrêt plus récent encore, dans lequel on ne trouve pas trace de la notion de communauté d'intérêts. Ainsi peut-on lire : « après avoir constaté que les propos litigieux avaient été diffusés sur le compte

445. - « (...) Inversement il ne faudrait pas exclure qu'une communauté d'intérêts soit décelable entre un grand nombre de personnes. La référence faite par le présent arrêt à un "nombre très restreint" de personnes accrédite sans doute cette approche d'une communauté d'intérêts sur les réseaux reposant sur la désignation, l'élection de quelques personnes par le titulaire du compte, qui ouvre ainsi à quelques happy few l'accès à ses messages » (A. Lepage, art. préc.).

446. - Cour d'appel de Versailles, 7 février 2018, n° 15/05739.

ouvert par la salariée sur le site facebook et qu'ils n'avaient été accessibles qu'à des personnes agréées par cette dernière et peu nombreuses, à savoir un groupe fermé composé de quatorze personnes, de sorte qu'ils relevaient d'une conversation de nature privée, la cour d'appel a pu retenir que ces propos ne caractérisaient pas une faute grave ; qu'exerçant le pouvoir qu'elle tient de l'article L. 1235-1 du code du travail, elle a décidé que le grief ne constituait pas une cause réelle et sérieuse de licenciement »⁴⁴⁷.

Les spécificités des communications numériques ne se limitent pas à exacerber les difficultés tenant à l'anonymat et à la confidentialité des messages, en matière d'expression personnelle. Elles favorisent une forme d'expression particulière par « relais », dont il faut à présent cerner les conséquences juridiques.

B - L'expression relayée

135. La mise en valeur des propos d'autrui - Une grande partie de l'activité des internautes consiste à attirer l'attention de ceux qui les lisent ou les écoutent sur des contenus créés par autrui et qui les auront intéressés, surpris, fait rire, choqués. Internet étant tout entier construit autour de la reproduction et du transfert d'information, les moyens techniques de cette mise en valeur des propos d'autrui sont simples et efficaces. Il y a certes longtemps qu'il est possible de conseiller à un collègue de bureau, à la machine à café, la lecture de tel article de journal repéré la veille. Mais le numérique change la donne, d'une part en offrant au partage un océan de contenus potentiellement illicites, d'autre part en permettant à l'internaute-relais de présenter à ceux qui le suivent un lien immédiatement cliquable, voire de reproduire le contenu concerné dans un espace virtuel dont il est responsable, sans effort et de manière instantanée. Cela ne va pas sans poser de délicates questions juridiques. Appeler sa centaine de contacts Facebook à regarder une vidéo diffamatoire, injurieuse ou incitant à la haine est-il constitutif d'une infraction pénale ? Relayer la diffamation, est-ce diffamer ; relayer l'injure, est-ce injurier ?

Il est nécessaire de distinguer certaines modalités techniques de partage, en tant qu'elles « mettent en scène » le propos relayé de diverses manières. Le relais est-il accompagné de commentaires personnels, manifeste-t-il implicitement ou expressément une adhésion ou, au contraire, une réprobation ? Ce n'est pas tout à fait la même chose que de créer un lien hypertexte (1), d'utiliser une fonction de republication sur un réseau social (2) ou d'utiliser un bouton visant à donner un « sentiment » sur un contenu (3).

447. - Cass. soc., 12 septembre 2018, n° 16-11690.

1. - La création d'un lien hypertexte

136. Quel statut juridique pour l'hyperlien ? - Le nom et le concept de « lien hypertexte » ont été inventés en 1965 par le sociologue américain Ted Nelson. Le terme « hyperlien » en constitue un synonyme. Il s'agit de transformer un texte « source » — ce peut également être une image — en élément interactif : l'internaute qui clique dessus est renvoyé vers une « cible », qui peut être une autre partie du document initialement consulté, mais aussi un document tiers figurant n'importe où sur Internet. C'est cette dernière hypothèse qui nous intéresse, en tant qu'elle permet au créateur d'un lien de diriger ses lecteurs vers des propos dont il n'est pas l'auteur. Que se passe-t-il si les propos cibles franchissent les limites de la liberté d'expression ? L'auteur du lien peut-il être traité comme s'il avait publié lui-même le texte auquel il renvoie ? La Cour suprême du Canada a été confrontée à cette question avant la Cour de cassation française, et y a apporté une réponse nettement plus détaillée⁴⁴⁸. Les motifs des juges du premier degré, des juges d'appel, l'opinion majoritaire et les opinions minoritaires publiées à cette occasion fournissent un très riche matériau de réflexion dont il faut donner ici un aperçu.

Un avertissement doit être formulé au préalable : Internet s'est bâti en grande partie sur la liberté d'interconnecter des contenus. Faire peser un risque juridique trop important sur la mise en place d'un lien reviendrait à pulvériser l'océan de l'information numérique en milliards de gouttelettes éparses. C'en serait fini du concept de « navigation » en ligne. Ni les êtres humains ni les robots des moteurs de recherche ne pourraient plus parcourir le réseau, et il faudrait connaître au préalable l'adresse exacte d'un contenu pour en prendre connaissance. C'est donc d'une main tremblante qu'il faut encadrer la pose de liens hypertextes, aussi bien sur le terrain de la liberté d'expression que sur celui de la propriété intellectuelle, ce dernier étant abordé plus loin⁴⁴⁹.

137. L'hyperlien comme « note de bas de page » neutre - Dans l'affaire canadienne, un lien avait été placé par une personne vers une page dont elle n'était pas l'auteur, mais qui contenait des propos potentiellement diffamatoires à l'égard d'un tiers. Les juges du premier degré avaient estimé que « (...) la simple création d'un hyperlien dans un site Web n'entraînait pas une présomption qu'on avait effectivement utilisé cet hyperlien pour accéder aux mots en cause. [...] les hyperliens s'apparentaient à des notes de bas de page puisqu'ils ne faisaient que renvoyer à une autre source sans toutefois en répéter le contenu. Sans répétition, il ne pouvait y avoir eu diffusion. Par surcroît, en l'absence de toute preuve établissant que qui que ce soit d'autre que C avait suivi les liens et lu les mots auxquels ils menaient, il était impossible de conclure qu'il y avait eu diffusion ».

448. - Cour suprême du Canada, *Crookes c. Newton*, 19 oct. 2011, 2011 CSC 47.

449. - V.infra, n° 216 s.

L'analogie avec la note de bas de page est très protectrice de l'auteur du lien. Le seul fait d'indiquer, dans un ouvrage papier, qu'il existe d'autres publications en rapport avec le propos n'est pas considéré à lui seul comme une quelconque forme d'adhésion à ces tiers écrits. Mais l'argument tiré de l'impossibilité de savoir si un internaute a effectivement suivi le lien ne convainc guère. Il est parfois possible techniquement de récupérer cette information, mais elle ne change rien au fond du problème. Une note de bas de page au pied d'un article universitaire ne cesse pas d'être neutre parce qu'un lecteur est allé consulter la référence proposée : c'est cette neutralité qui commande l'analyse.

La Cour suprême approfondit le raisonnement. L'opinion majoritaire est que :

Les hyperliens constituent essentiellement des renvois, qui diffèrent fondamentalement d'autres actes de « diffusion ». Tant les hyperliens que les renvois signalent l'existence d'une information sans toutefois en communiquer eux-mêmes le contenu. Ils obligent le tiers qui souhaite prendre connaissance du contenu à poser un certain acte avant de pouvoir le faire. Le fait qu'il soit beaucoup plus facile d'accéder au contenu d'un texte par le biais d'hyperliens que par des notes de bas de page ne change rien au fait que l'hyperlien en lui-même est neutre sur le plan du contenu. En outre, le seul fait d'incorporer un hyperlien dans un article ne confère pas à l'auteur de celui-ci un quelconque contrôle sur le contenu de l'article secondaire auquel il mène.

Une des clés de compréhension de la matière serait donc l'absence de reproduction du contenu lié à l'intérieur de la page source. Le lien n'amène pas le contenu cible sous les yeux du lecteur, qui doit prendre l'initiative d'aller récupérer le document, même s'il n'a qu'un clic à faire pour cela. Il faut garder à l'esprit que les juges raisonnent à partir du problème de la diffamation, infraction qui repose en effet, y compris en droit français, sur la notion de reproduction : les textes visant la « diffusion », concept plus large, obéissent comme on le verra à une logique différente⁴⁵⁰.

La Cour suprême est donc d'avis qu'un lien hypertexte est « neutre sur le plan du contenu ». Toutefois, à suivre certains des juges canadiens, cette neutralité pourrait être remise en question de deux façons : lorsque l'auteur du lien y adjoint certains commentaires ; lorsque l'auteur prête au lien certaines caractéristiques techniques.

138. La neutralité remise en question par le commentaire - Les juges d'appel avaient expliqué « qu'il pouvait arriver que certains mots d'un article donnent à penser qu'un hyperlien donné constitue un encouragement ou une invitation à se rendre au site visé, mais ce n'était pas le cas en l'espèce ». Au niveau de la Cour suprême, deux juges minoritaires adoptent une ligne similaire, en écrivant : « Cependant, selon nous, l'hyperlien équivaut à de la diffusion s'il ressort du

450. - V.infra, n°141.

texte qui le contient, interprété en fonction de son contexte, que l’auteur adopte le contenu auquel il renvoie, ou y adhère »⁴⁵¹.

L’analyse est convaincante, et compatible avec « l’analogie de la note de bas de page ». Lorsque ladite note contient une simple référence, elle peut s’interpréter comme contenant le sous-texte suivant : « la lecture de ce document éclaire le sujet abordé et participe à son appréhension exhaustive ». Cela ne marque ni approbation ni réprobation avec le contenu en cause, mais dresse un simple constat d’utilité de sa consultation. Citer *Mein Kampf* comme un document dont la lecture éclaire l’Histoire de la Deuxième Guerre mondiale ne signifie évidemment pas rejoindre le point de vue d’Hitler. Mais ce silence valant sous-texte implicite peut, à la discrétion de l’auteur de la note de bas de page ou du lien hypertexte, être remplacé par un commentaire dévoilant le rapport personnel qu’il entretient avec la ressource ciblée. Encore distinguerons-nous la formulation des juges d’appel de celle des juges minoritaires de la Cour suprême. Un « encouragement à se rendre au site visé » ne revient toujours pas à endosser le propos, et ne diffère d’ailleurs pas substantiellement d’une note de bas de page ou d’un lien silencieux. Pourquoi indiquer une référence, si ce n’est pour inviter à sa consultation ? En revanche, un propos manifestant une « adoption » ou une « adhésion » revient bien à ce que l’auteur du lien répète les propos cibles, et doive alors les assumer devant la loi comme s’il les avait lui-même prononcés ou écrits.

Le raisonnement qui vient d’être décrit est compatible avec une décision rendue, en France, par la Cour de cassation⁴⁵². Un article de blog contenait un lien vers une vidéo, dont l’auteur du blog n’était pas l’auteur et qui contenait des menaces de mort. La Chambre criminelle juge que :

*[...] le renvoi par un lien hypertexte à une vidéo contenant des menaces de mort proférées par des tiers n’est pas susceptible de constituer, à lui seul, la commission par le prévenu de l’infraction prévue par l’article 433-3 du code pénal*⁴⁵³.

Dire que le lien n’est pas suffisant « à lui seul » signifie bien qu’une adjonction d’éléments pourrait conduire à retenir l’incrimination pénale. Un commentaire révélant une adhésion au propos ciblé constituerait certainement le supplément attendu. Mais la neutralité de principe du lien peut-elle être remise en cause d’une autre façon ?

451. - Opinion de la Juge en chef McLachlin et du Juge Fish.

452. - On fait prudemment état d’une motivation « compatible » et non identique, car la Cour de cassation ne livre pas au lecteur les ressorts profonds de sa décision. La différence entre les techniques anglo-saxonne et française de motivation est, comme souvent, frappante.

453. - Cass. crim., 31 mars 2016, n° 15-82.417.

139. La neutralité remise en question par la technique ? - Une autre juge minoritaire de la Cour suprême du Canada estime qu'il existe plusieurs catégories distinctes de lien hypertexte, et qu'elles ne peuvent pas être traitées de la même façon.

Pour décider si l'information à laquelle mène un hyperlien est immédiatement disponible, le tribunal doit prendre en considération certains facteurs, notamment s'il s'agit d'un hyperlien activé par l'utilisateur ou automatique, s'il s'agit d'un lien superficiel ou profond, et si l'information à laquelle mène le lien est accessible au grand public (ou s'il s'agit plutôt d'un contenu à accès restreint). Tout ce qui a une incidence sur la facilité avec laquelle on peut prendre connaissance des propos en cause sera pertinent à cet égard⁴⁵⁴.

Un lien superficiel est un lien qui renvoie à la page d'un site, alors qu'un lien profond pointe vers une ressource précise. Il est difficile de comprendre quel rôle il faudrait faire jouer à cette distinction. Les raisonnements menés jusqu'ici l'étaient sur la base d'un lien profond, menant vers des propos particuliers et non vers la racine d'une page Internet. Pointer vers un document donné reste, au premier abord, un acte neutre. Le fait que la ressource liée soit à accès public ou restreint ne semble pas non plus fondamental : elle n'a d'impact que sur le degré de motivation nécessaire au lecteur pour prendre connaissance du document cible. S'il faut s'inscrire, voire payer pour le faire, cela est plus pénible que s'il suffit d'un clic. Accepter un tel raisonnement remet totalement en question la différence entre une note de bas de page « papier » — qui suppose, dès qu'elle ne constitue pas un renvoi interne à l'ouvrage consulté, d'importants efforts pour accéder à la référence — et le lien hypertexte, en posant que la différence de confort et de célérité entraîne une différence de nature. Cela ne semble pas souhaitable. En revanche, la Juge mentionne l'existence de liens automatiques, c'est-à-dire de liens qui s'ouvriraient sans que l'utilisateur n'ait de démarche pas à accomplir. La question peut être rapprochée des liens que certains réseaux sociaux transforment automatiquement en aperçus, notamment les liens vers des images ou des vidéos. Dans ces situations, lier un contenu équivaut quasiment à le reproduire⁴⁵⁵. Cette difficulté liée à la reproduction du contenu illicite se retrouve dans les fonctions de partage, qu'il faut à présent aborder.

2 - Les fonctions de partage des réseaux sociaux

140. La diffusion pyramidale de l'information - Les informations qui intéressent un nombre suffisant d'internautes circulent à une vitesse inouïe sur les réseaux sociaux. Cela ne doit rien au hasard : l'architecture de ces plateformes a été spécifiquement pensée pour faciliter autant que

454. - Opinion de la Juge Deschamps.

455. - Cela produit des conséquences en droit de la propriété intellectuelle : V.infra, n°218.

possible cette propagation. Lorsqu'une personne découvre dans son fil d'actualités un contenu drôle, intéressant ou choquant, elle n'a que deux clics à faire pour la partager avec ses contacts. Ceux-ci la verront à leur tour apparaître dans l'interface de leur réseau et auront la possibilité de la partager à nouveau. Ce modèle pyramidal permet à une information « virale » d'apparaître sur des millions d'écrans en l'espace de quelques minutes seulement. Twitter, en particulier, est conçu comme épure entièrement centrée sur cette fonction de partage, où elle prend nom de « retweet » (usuellement abrégé en « RT »). Sur ce réseau, les internautes choisissent de s'abonner au fil d'actualités d'une personne ou d'une institution donnée non seulement pour la qualité des messages qu'elle rédige personnellement, mais aussi — et parfois surtout — pour la qualité de ses retweets. Le compte suivi est ainsi plébiscité pour son rôle de vigie informationnelle, pour son aptitude à repérer, sélectionner et relayer des contenus conformes aux attentes de ses abonnés. Or, parmi les informations qui circulent sur ces plateformes, le meilleur côtoie le pire. Au moment d'un attentat, la puissance de ces réseaux a parfois porté sous les yeux de tous les appels à l'aide de victimes, et permis d'y répondre. Des citoyens ordinaires ont ouvert leurs portes et offert soins et abri à de parfaits inconnus. Mais Twitter et Facebook ont aussi charrié des injures racistes d'une rare violence et des appels aux meurtres. Ils ont aussi été les véhicules de rumeurs trompeuses et infondées : si les médias traditionnels sont plus lents à réagir, c'est aussi parce qu'ils prennent le temps d'effectuer des vérifications. Les simples internautes, qui n'y procèdent pas toujours, sont victimes d'erreurs, et parfois instruments ou instigateurs de manipulations pures et simples de l'opinion.

Il semble alors évident que le droit ne peut se désintéresser du geste qui consiste à relayer l'information reçue d'autrui. Aux raisons d'opportunité qui viennent d'être décrites, s'ajoute une considération technique : contrairement à la mise en place d'un simple lien hypertexte, ces fonctions de partage emportent reproduction de tout ou partie du contenu d'origine. Il ne s'agit plus de référencer des propos, de proposer une simple « note de bas de page », mais bien de les diffuser. Quelles conséquences juridiques faut-il attacher à cet acte ?

141. Les textes réprimant explicitement les actes de diffusion - À la suite de notre première publication destinée au grand public et évoquant la possibilité de réprimer pénalement un simple partage sur les réseaux sociaux, de nombreux internautes nous ont fait part de leur stupeur⁴⁵⁶. La rapidité et l'apparente passivité de l'acte de partage paraissaient incompatibles, dans leur esprit, avec une éventuelle qualification pénale assortie de peines de prison ferme. Cette illusion peut être rapidement dissipée en mobilisant un exemple radical : le seul fait de participer à la diffusion d'images à caractère pédopornographique fait encourir les mêmes peines que le fait d'avoir

456. - « Les conséquences juridiques du retweet », article du 14 décembre 2012, sur *unpeuedroit.fr*. Il s'agit d'un article de vulgarisation, principalement destiné à des non-juristes.

enregistré ou fixé de telles images⁴⁵⁷. Mais d'autres textes bien plus anodins répriment, outre la publication d'une information, le simple fait d'avoir participé à sa diffusion. Ainsi l'interdiction de publier des sondages la veille et le jour de certaines élections est-elle assortie de l'interdiction de diffuser de tels sondages⁴⁵⁸. Par ailleurs, la notion de « diffusion » est si large qu'il est probable que même la pose d'un lien hypertexte tombe sous le coup de telles incriminations. Il en va autrement quand c'est la « reproduction » qui est visée. C'est le cas en matière de diffamation, infraction qui mérite d'être spécifiquement étudiée en raison du rôle-clé qu'elle joue dans l'équilibre français en matière d'expression publique.

142. La diffamation par simple reproduction - Il faut reconnaître à M. Jérôme Cahuzac le mérite d'avoir stimulé la réflexion des chercheurs en droit du numérique. Le 4 décembre 2012, le ministre du Budget envoie deux messages sur le réseau social Twitter. Le premier fait allusion à l'article de Mediapart l'accusant de détenir un compte bancaire à l'étranger et de l'avoir caché au fisc français. Le deuxième tweet est ainsi libellé : « Je poursuivrai tous ceux qui reprendront cette calomnie gravement diffamatoire et qui porte atteinte à mon honneur. Y compris ici ! »⁴⁵⁹.

« Ici » : sur le réseau. « Retweeter » des propos diffamatoires serait une diffamation ? L'avertissement n'est pas infondé. L'article 29 de la loi de 1881 dispose en effet :

*Toute allégation ou imputation d'un fait qui porte atteinte à l'honneur ou à la considération de la personne ou du corps auquel le fait est imputé est une diffamation. La publication directe **ou par voie de reproduction** de cette allégation ou de cette imputation est punissable, **même si elle est faite sous forme dubitative***⁴⁶⁰.

Affirmer, comme le faisait Mediapart, que le ministre du Budget avait dissimulé de l'argent aux services fiscaux était certainement attentatoire à son honneur. Dès lors, le simple fait de répercuter cette accusation tombe sous le coup du texte. Le fait d'assortir l'acte de partage d'un commentaire personnel exprimant une incertitude sur la réalité de l'information ne suffit même pas à éviter les

457. - Art. 227-23 C. pén. : « Le fait, en vue de sa diffusion, de fixer, d'enregistrer ou de transmettre l'image ou la représentation d'un mineur lorsque cette image ou cette représentation présente un caractère pornographique est puni de cinq ans d'emprisonnement et de 75 000 euros d'amende. Lorsque l'image ou la représentation concerne un mineur de quinze ans, ces faits sont punis même s'ils n'ont pas été commis en vue de la diffusion de cette image ou représentation. Le fait d'offrir, de rendre disponible ou **de diffuser une telle image ou représentation, par quelque moyen que ce soit**, de l'importer ou de l'exporter, de la faire importer ou de la faire exporter, est puni des mêmes peines [...] ». Nous soulignons.

458. - Art. 11 de la loi n° 77-808 du 19 juillet 1977 relative à la publication et à la diffusion de certains sondages d'opinion : « En cas d'élections générales et de référendum, la veille et le jour de chaque scrutin, aucun sondage électoral ne peut faire l'objet, par quelque moyen que ce soit, d'une publication, d'une diffusion ou d'un commentaire [...] ».

459. - Le tweet a été ultérieurement supprimé par son auteur, pour d'assez évidentes raisons, mais un moteur de recherche permet de retrouver en un instant l'une des nombreuses captures d'écran réalisées par des internautes.

460. - Nous soulignons.

foudres de la loi ! Cette solution, qui semble bien sévère au premier abord, se comprend par la préoccupation qui animait certainement le législateur : empêcher la propagation de rumeurs nauséabondes. Partager l'accusation dégradante, c'est lui donner corps et substance, la porter à l'attention d'autrui, quand bien même le véhicule serait habillé d'incertitude. Le combat contre la rumeur, légitime déjà au XIXe siècle, n'est que plus nécessaire à présent qu'un ragot peut faire le tour du monde en moins d'une heure.

Encore faut-il permettre aux citoyens de débattre entre eux de sujets d'intérêt public, et la probité des responsables politiques et des élus en fait certainement partie⁴⁶¹. Il faut donc rappeler qu'une fois la diffamation caractérisée, certains moyens de défense sont accessibles à la personne mise en cause. L'accès à ces excuses ne doit pas être trop difficile ou trop étroit, sans quoi le débat démocratique serait menacé. Tout individu poursuivi pour diffamation peut soulever deux moyens de défense spécifiques à cette incrimination. Le premier est consacré par la loi : c'est l'« *exception de vérité* », qui consiste à démontrer la réalité des faits relatés. L'individu qui n'a pas colporté un ragot, mais simplement révélé ou rappelé un fait objectif n'est pas inquiété⁴⁶². Mais au moment où M. Cahuzac menaçait les internautes de poursuites, son attirance coupable pour le tourisme fiscal n'avait pas encore été démontrée de manière irrévocable. Restait alors le second moyen de défense, d'invention prétorienne : la preuve de la bonne foi. Sera considéré comme s'étant exprimé de bonne foi, même s'il ne peut démontrer avec certitude la véracité de ses allégations attentatoires à l'honneur ou à la considération de la personne, celui qui répondra à quatre conditions : « *le fait justificatif de bonne foi distinct de l'exception de vérité des faits diffamatoires se caractérise par la légitimité du but poursuivi, l'absence d'animosité personnelle, la prudence et la mesure dans l'expression ainsi que par le sérieux de l'enquête* »⁴⁶³. Le dernier de ces quatre critères, qui fait référence à une « enquête », révèle que l'excuse de bonne foi a été pensée pour les professionnels de l'information. Assigné en diffamation, Mediapart aurait dû livrer des éléments d'investigation précis et solides. Mais le juge a su, par la suite, adapter cette exigence à la situation de citoyens

461. - La Cour européenne des Droits de l'Homme est particulièrement vigilante face aux atteintes à la liberté d'expression, décidées par les législations nationales, mais qui feraient obstacles à des débats d'intérêt général : V. X. Boy, « Conv. EDH, art. 10 : liberté d'expression et de la presse » in *Répertoire Dalloz de droit européen*, n° 77 s. ; B. Beignier, B. de Lamy et E. Dreyer (dir), *Traité de droit de la presse et des médias*, op. cit., n° 199 s. La liberté d'expression doit être interprétée de manière particulièrement large lorsqu'elle est employée pour critiquer le comportement du personnel politique. Pour un ex. récent, V. CEDH, 17 mars 2017, *Olfasson c. Islande*, req. n° 58493/13.

462. - Art. 35 de la loi de 1881. Le texte précise cependant : « (...) La vérité des faits diffamatoires peut toujours être prouvée, sauf : a) Lorsque l'imputation concerne la vie privée de la personne ; b) Lorsque l'imputation se réfère à des faits qui remontent à plus de dix années ; c) Lorsque l'imputation se réfère à un fait constituant une infraction amnistiée ou prescrite, ou qui a donné lieu à une condamnation effacée par la réhabilitation ou la révision (...) ».

463. - Expression que l'on retrouve par ex. dans Cass. 1ère civ., 17 mars 2011, n° 10-11784 : Bull. civ., I, n° 58.

ordinaires. À propos d'un blogueur, le TGI de Paris a ainsi jugé que : « si l'auteur d'un blog n'est pas tenu d'avoir procédé préalablement à une enquête sérieuse empreinte d'un effort d'objectivité, telle qu'elle est attendue d'un journaliste professionnel participant à l'information du public, [il] ne saurait se dispenser pour autant de justifier qu'il détenait des éléments sérieux donnant quelque crédit à ses affirmations »⁴⁶⁴. Il pourrait dès lors être reproché au quidam d'avoir propagé des rumeurs sans source identifiée, ou dont la source ne présente aucune garantie de sérieux. En revanche, le fait qu'un média réputé lance des accusations argumentées contre une personnalité publique devrait suffire à ce que les citoyens soient autorisés à propager l'information - à supposer que les autres conditions du fait justificatif de bonne foi soient réunies, notamment « l'absence d'animosité personnelle ».

143. Les autres limites à la liberté d'expression - De nombreuses incriminations punissant des abus de la liberté d'expression n'évoquent ni les actes de diffusion ni les actes de reproduction de propos illicites. À titre de simples exemples, on peut citer l'injure⁴⁶⁵, l'incitation à la haine⁴⁶⁶ ou encore la négation de crime contre l'Humanité⁴⁶⁷. À chaque fois que des propos constitutifs de telles infractions sont relayés, le trouble social risque d'augmenter. Mais, en réalité, il existe des raisons diverses et antagonistes de transférer à ses contacts de telles informations. Peut-être s'agit-il de marquer implicitement une adhésion. Mais il peut être aussi question de pointer du doigt un propos initial jugé abominable. Le « retweet » ou le « partage » d'un propos raciste ne sera pas interprété de la même manière selon qu'il émane d'un proche de l'extrême droite ou de la LICRA. En matière de diffamation, nous avons vu que le transport du message est réprimé pour lui-même, et nous avons dit pourquoi. Ce n'est pas le cas du relais d'un propos injurieux ou raciste : s'il est accompagné d'une prise de distance, d'une dénonciation, d'une défense de la victime, il ne heurte pas les valeurs sociales protégées par l'incrimination. Le juge devra rechercher les éléments de contexte propres à éclairer l'intention de l'internaute-relais. Dans des cas exceptionnels, dont

464. - Tribunal de grande instance de Paris 17e chambre Jugement du 16 octobre 2006, *Nissan Europe et autres / Stéphanie G.*

465. - Art. 29 al. 2 de la loi de 1881 précitée : « Toute expression outrageante, termes de mépris ou invective qui ne renferme l'imputation d'aucun fait est une injure ».

466. - Art. 24 al. 7 de la loi de 1881 précitée : « Ceux qui, par l'un des moyens énoncés à l'article 23, auront provoqué à la discrimination, à la haine ou à la violence à l'égard d'une personne ou d'un groupe de personnes à raison de leur origine ou de leur appartenance ou de leur non-appartenance à une ethnie, une nation, une race ou une religion déterminée, seront punis d'un an d'emprisonnement et de 45 000 euros d'amende ou de l'une de ces deux peines seulement ».

467. - Art. 24 bis al. 1 de la loi de 1881 précitée : « Seront punis d'un an d'emprisonnement et de 45 000 € d'amende ceux qui auront contesté, par un des moyens énoncés à l'article 23, l'existence d'un ou plusieurs crimes contre l'humanité tels qu'ils sont définis par l'article 6 du statut du tribunal militaire international annexé à l'accord de Londres du 8 août 1945 et qui ont été commis soit par les membres d'une organisation déclarée criminelle en application de l'article 9 dudit statut, soit par une personne reconnue coupable de tels crimes par une juridiction française ou internationale ».

l'exemple imaginaire de la LICRA ferait probablement partie, un partage sans commentaire ne créerait pas de risque de condamnation : l'identité même du relais donne un sens particulier à l'acte. Le reste du temps, les internautes auraient tort de considérer que leur intention est évidente. Elle l'est pour eux et pour ceux qui les connaissent bien, mais cela n'est pas suffisant lorsque leur partage est public⁴⁶⁸. À défaut de tout indice révélant une prise de distance, le juge serait bien fondé à considérer que l'internaute a fait sien le propos relayé. Il ne s'agit pas d'une présomption de culpabilité : répéter des mots de haine sans démontrer qu'on l'a fait pour de justes motifs, c'est créer le même trouble à l'ordre public que l'auteur initial⁴⁶⁹. De plus, si le juge se montrait trop clément, une fraude commode consisterait à s'exprimer à travers une reprise sans commentaire d'anciens messages illicites rédigés par autrui. Sur Twitter, par exemple, il suffirait de lancer une recherche par mot-clé pour tomber inmanquablement sur n'importe quel type de propos injurieux ou incitant à la haine à l'encontre de minorités, de religions ou d'orientations sexuelles : la bibliothèque de l'horreur y est déjà d'une infinie richesse. Il suffirait alors de partager des messages vieux de quelques années pour s'assurer une totale impunité. Cela reviendrait à hurler des propos antisémites dans la rue en prétendant citer un vieux livre. Dans certains contextes, la prétendue diffusion est un procédé grossier qui dissimule mal l'adhésion personnelle au propos initial : il faut alors en assumer les conséquences. Quels sont ces contextes ? Pour frustrante que soit cette réponse, il n'est pas possible de le déterminer de manière abstraite.

Précisons enfin que, lorsqu'il recherche les éléments de contexte propres à marquer une prise de distance ou une dénonciation relayée, le juge ne devrait attacher qu'une importance faible ou nulle aux clauses générales que l'on voit fleurir, sur Twitter notamment, dans les descriptions de comptes utilisateurs : « mes RT ne valent pas approbation »⁴⁷⁰. Chacun, lorsqu'il relaie des propos par hypothèse illégaux, doit prendre la peine d'expliquer son intention au cas par cas, et nul ne peut prétendre s'exonérer de cette obligation par une clause générale.

468. - Une recherche sur Twitter sur les mots « *no comment* », à n'importe quel moment fournira au curieux un échantillon de propos relayés accompagnés simplement de ces deux mots. Il s'agit généralement de marquer une approbation ou une désapprobation si fortes que le sens est supposé évident pour tous. Il ne l'est pas toujours.

469. - Lorsqu'une injure est relayée par un média, y compris en ligne - hypothèse très proche de celle qui nous occupe, le raisonnement est le suivant : « En cas de publication indirecte, c'est-à-dire lorsque la transmission au public est assurée par un tiers (média), cette preuve est simplifiée. La démarche de l'auteur du propos n'est vérifiée que pour s'assurer de son caractère injurieux. En toute hypothèse, elle ne coïncide pas avec l'élément moral de l'infraction qui est, lui, établi par voie de présomption : le directeur de la publication ou l'éditeur assume une responsabilité de plein droit. Il est nécessairement responsable d'une telle publication dès lors qu'il avait pour mission de vérifier les contenus diffusés par son intermédiaire et de les expurger de tout contenu infractionnel. En laissant publier un propos injurieux, il a accepté de se voir reprocher une telle publication » (E. Dreyer, « Injures publiques et non publiques », *in Rép. pén. Dalloz*, févr. 2017, n° 176).

470. - Sur ce point : A. Mirsky et K. Tummarello, « Are Retweets Endorsements?: Disclaimers and Social Media », article *dmlp.org* du 4 mai 2012.

Cette difficulté qui tient à l'ambiguïté de l'acte de partage ne se retrouve pas — imagine-t-on — lorsque le bouton utilisé pour réagir au propos initial est précisément conçu pour indiquer un état d'esprit ou une émotion.

3 - Les boutons exprimant une « émotion » face à un contenu

144. **Un partage assorti de commentaire** - Certains réseaux sociaux proposent, à côté d'une fonction neutre de « partage », l'expression d'un sentiment par l'internaute face au contenu qui lui est présenté. Le bouton « j'aime » du réseau social Facebook en constitue le plus célèbre exemple. Depuis 2016, une palette de réactions plus variée est offerte aux utilisateurs, qui peuvent indiquer non seulement « j'aime », mais encore « j'adore », « haha », « wouah », « triste » et « grrr ». Résistons à la tentation de déduire de ces onomatopées le niveau de vocabulaire que le réseau social prête à ses utilisateurs, et interrogeons-nous sur les conséquences juridiques d'un clic sur ces différents boutons. À cet égard, une intéressante décision d'une Cour américaine mérite d'être citée. Des employés du bureau Shériff d'Hampton, Virginie, avaient été licenciés pour avoir cliqué sur le bouton « j'aime » de la page Facebook de l'opposant à l'actuel Shériff. Une partie du litige porta sur le point de savoir si leurs clics pouvaient être interprétés comme une forme d'expression protégée par le Premier amendement à la Constitution des États-Unis d'Amérique⁴⁷¹. La Cour d'appel du quatrième circuit apporta cette réponse limpide :

On the most basic level, clicking on the “like” button literally causes to be published the statement that the User “likes” something, which is itself a substantive statement. In the context of a political campaign’s Facebook page, the meaning that the user approves of the candidacy whose page is being liked is unmistakable. That a user may use a single mouse click to produce that message that he likes the page instead of typing the same message with several individual key strokes is of no constitutional significance. Aside from the fact that liking the Campaign Page constituted pure speech, it also was symbolic expression. The distribution of the universally understood “thumbs up” symbol in association with Adams’s campaign page, like the actual text that liking the page produced, conveyed that Carter supported Adams’s candidacy⁴⁷².

Ces boutons doivent donc être considérés comme strictement équivalents à un partage accompagné d'un texte de type « j'aime » ou « cela me fait rire ». Voilà qui pourrait dissiper l'équivoque d'un acte de partage « sec », et constituer l'approbation — ou, à l'inverse, la condamnation — du propos initial nécessaire au bon traitement juridique du relais. Ainsi, lorsque M. Dieudonné Mbala Mbala est condamné pour avoir publié un statut Facebook constitutif

471. - Les différentes pièces du dossier sont consultables sur la page *Bland v. Roberts* du *Digital Media Law Project* : <http://www.dmlp.org/threats/bland-v-roberts>.

472. - États-Unis, Richmond 4th circuit Court, 18 sept. 2013, *Bland v. Roberts*, Appeal n°12-1671, p. 39.

d'apologie du terrorisme, on ne voit pas d'obstacle théorique à la poursuite des internautes ayant « aimé » ledit statut⁴⁷³.

145. **L'ambiguïté persistante** - Si l'exemple qui vient d'être pris paraît clair, il n'en va pas toujours ainsi. Dans une précédente publication, nous relevions qu'un millier de personnes avaient « aimé », sur Facebook, un article du journal Le Monde intitulé « Argentine : plusieurs Français tués après une collision entre hélicoptères »⁴⁷⁴. Voudraient-elles saluer ainsi la réactivité du journal ? Féliciter les auteurs pour la clarté de l'article, ou pour son style ? Montrer leur soutien aux victimes ou à leurs familles ? Ou, hypothèse terrible, se réjouissaient-elles de cet accident ? À l'époque, il n'était possible que de « partager » l'article — réaction que d'aucuns jugeaient peut-être trop froide — ou de « l'aimer » - au risque de donner à ce mot tous les sens différents, voire incompatibles qui viennent d'être imaginés. La signification du relais associé à une « émotion » n'est donc pas toujours claire, ce qui peut poser problème lorsque l'adhésion ou la prise de distance doivent être recherchées⁴⁷⁵. En multipliant les « émotions » susceptibles d'être exprimées, Facebook réduit théoriquement les risques d'équivoque. Cette clarification des sentiments éprouvés par ses utilisateurs à l'égard des contenus rencontrés a probablement été permise moins pour leur confort que pour collecter des données personnelles toujours plus fines qui pourront être ensuite monnayées à des tiers⁴⁷⁶. Mais elle permettra peut-être aussi au juge d'y voir plus clair⁴⁷⁷.

Toutes les difficultés qui viennent d'être examinées, s'agissant du relais de l'expression d'autrui sur Internet, peuvent se cumuler : un internaute A publie un lien qui pointe vers une page Web contenant des propos diffamatoires ; B partage la publication de A ; C déclare qu'il « aime » ce partage. Plus le lien entre l'utilisateur de réseau social et le contenu illicite sera distendu, plus il faudra faire preuve de prudence avant de le traiter comme s'il avait directement adhéré à ce contenu ou comme s'il en était l'auteur.

473. - La Cour d'appel de Paris l'a condamné, le 21 juin 2016, à 2 mois de prison avec sursis et 10 000 euros d'amende pour avoir écrit, quelques jours après les attentats dits « de Charlie Hebdo » : « je me sens Charlie Coulibaly ». Coulibaly était le nom porté par les terroristes.

474. - Article du 9 mars 2015, développé dans l'article précité « La liberté d'expression sur les réseaux sociaux en droit français ».

475. - V.supra, n°143.

476. - Sur cette question, V. not.supra, n° 50 et s.

477. - L'optimisme sur ce point se doit d'être modéré. Un bouton comme « waouh » (accompagné d'un symbole de bouche ouverte) n'a pas de signification claire. Et il sera toujours possible pour l'internaute d'affirmer, comme on l'a suggéré, qu'il « adore » non pas l'agression homophobe relatée par tel article, mais la manière dont cet article est rédigée. C'est le problème d'une expression sous forme de dessins ou d'onomatopées : sa grande pauvreté rend son sens difficile à percevoir, et le risque existe que certains en tirent parti. Cherchant à renouveler l'expérience conduite sur un article du Monde relatant une catastrophe, à présent qu'une variété d'icônes existe, il nous faut en tout cas constater que sur le titre « Chine : les Français appelés à la vigilance après une agression » (31/03/17), une trentaine d'internautes clique sur « j'aime », une vingtaine sur « ahah » et seulement 7 sur « grrr ».

À présent que les difficultés considérables qui touchent à la détermination des expressions illicites en ligne ont été présentées, il est temps d'aborder les difficultés touchant aux sanctions, qui sont d'un autre ordre.

II - Les difficultés tenant à la sanction de l'expression illicite

146. **Plan** — Supposons l'illicéité du propos caractérisée — soit qu'elle ait été manifeste dès l'origine, soit que les difficultés de qualification précédemment évoquées aient surgi, mais aient été surmontées -, il reste à en punir l'auteur. La brièveté des délais de prescription (A) et l'abondance de contenus illicites (B) se combinent toutefois pour rendre les sanctions fort rares en pratique.

A - La brièveté des délais de prescription

147. **Les prescriptions spéciales du droit de la presse** - Une grande partie des règles encadrant la liberté d'expression dans notre droit est issue de la loi de 1881⁴⁷⁸. Alors que la prescription de l'action publique pour les délits de droit commun est fixée à six ans⁴⁷⁹, le droit de la presse prévoit un délai de principe extrêmement bref :

*L'action publique et l'action civile résultant des crimes, délits et contraventions prévus par la présente loi se prescriront après trois mois révolus, à compter du jour où ils auront été commis ou du jour du dernier acte d'instruction ou de poursuite s'il en a été fait*⁴⁸⁰.

Par exception, la loi de 1881 prévoit un délai de prescription d'un an s'agissant de certaines infractions considérées comme particulièrement ignobles⁴⁸¹. En revanche, elle ne pose aucune règle particulière en considération de la nature du support de publication. Certains l'ont regretté, et ont proposé de modifier la loi applicable à la première publication numérique (1). La jurisprudence a dû

478. - Une grande partie, mais pas toutes. Ainsi la provocation au terrorisme et l'apologie du terrorisme ont-ils été « sortis » de la loi sur la liberté de la presse pour intégrer le Code pénal (art. 421-2-5), ce qui a entre autres pour effet de faire échapper cette infraction à la courte prescription ici évoquée. La tentation sera grande, pour le législateur, d'extirper à l'avenir d'autres abus de la liberté d'expression du régime spécial pour leur faire intégrer le droit commun. La Commission nationale consultative des Droits de l'Homme, dans un *Avis sur la lutte contre les discours de haine sur Internet* du 12 février 2015, (<http://www.cncdh.fr/fr/publications/avis-sur-la-lutte-contre-les-discours-de-haine-sur-internet>) met en garde contre la tentation de restreindre trop largement la liberté d'expression.

479. - Art. 8 du Code de procédure pénale. Ce délai est issu de la loi n° 2017-242 du 27 février 2017 portant réforme de la prescription en matière pénale. Il était auparavant de trois années.

480. - Art. 65 al. 1 de la loi de 1881 précitée.

481. - En vertu de l'article 65-3 de la même loi, le délai est porté à un an pour la provocation à la haine ou à la violence, l'injure ou la diffamation à l'égard de certaines personnes ou groupes de personnes (en raison de leur ethnie, religion, sexe...) ; pour la contestation d'existence de crimes contre l'humanité.

par ailleurs se pencher sur des situations dans lesquelles une mise en valeur de la publication initiale valait nouvelle publication, ce qui entraîne le départ d'un nouveau délai de prescription (2).

1 - La prescription applicable à la publication initiale

148. Un point de départ spécial pour les supports numériques ? - Le point de départ habituel de la prescription est classiquement constitué par le premier acte de publication⁴⁸². Mais la Cour d'appel de Paris a refusé d'appliquer cette solution en matière d'écrits numériques, aux motifs que :

[...] si la mise en œuvre de ce principe est aisément applicable à des messages périssables, voire furtifs, dès lors qu'ils ont fait l'objet d'une publication sur support papier ou audiovisuel, il n'en va pas de même lorsque le message a été publié sur Internet qui constitue un mode de communication dont les caractéristiques techniques spécifiques obligent à adapter les principes posés par la loi sur la presse ; [...] Dans l'hypothèse d'une publication sur Internet, la publication résulte de la volonté renouvelée de l'émetteur qui place le message sur un site et choisit de l'y maintenir ou de l'en retirer quand bon lui semble ; [...] L'acte de publication devient ainsi continu et cette situation d'infraction inscrite dans la durée est d'ailleurs une notion de droit positif en droit pénal où elle s'applique dans l'incrimination de plusieurs délits ; [...] Dès lors, il y a lieu de considérer qu'en choisissant de maintenir accessible sur son site les textes en cause aux dates où il a été constaté que ceux-ci y figuraient, et à la date du jugement civil en première instance, le prévenu a procédé à une nouvelle publication ce jour-là et s'est exposé à ce que le délai de prescription de trois mois court à nouveau à compter de cette date⁴⁸³.

En d'autres termes, l'acte de publier aurait une nature profondément différente selon les supports. Dans les cas de la presse ou de l'audiovisuel, il s'accomplit en un instant précis : celui où le journal est placé sur les rayonnages d'un kiosque ou dans les boîtes aux lettres des abonnés ; celui où l'émission de télévision ou de radio est lancée sur les ondes. Ce relâchement passé, l'éditeur du support s'en désintéresserait, en quelque sorte, ou du moins le laisserait vivre sa vie propre. En ligne, en revanche, derrière chaque publication, il faudrait déceler en coulisses la volonté tendue et sans cesse renouvelée de l'éditeur de lancer son contenu à la face du monde.

En réalité, le responsable d'un hebdomadaire papier a peut-être clairement présent à l'esprit ce numéro paru il y a cinq ans, auquel il songe avec fierté et dont il assume volontiers le contenu. L'éditeur d'un site, l'auteur d'un blog ou d'un message sur Twitter a pu quant à lui lancer sur la toile un contenu qui lui semblait anodin, au milieu de centaines d'autres, et l'oublier rapidement sans qu'il cesse pour autant d'être consultable. Le raisonnement de la Cour d'appel de Paris repose sur un non-dit. Ce qui sépare ces situations, ce qui différencie le support classique du support en ligne, c'est la faculté qui existe dans le second cas, mais non dans le premier, d'exercer un droit de

482. - Par ex. Cass. crim., 13 oct. 1987, n° 86-96686 : Bull. crim., n° 349.

483. - CA Paris, 11e ch. corr., 15 déc. 1999, n° XP151299X.

remords, de retirer la publication. Il n'est pas au pouvoir du journal de faire disparaître les numéros des placards de ses abonnés, tandis qu'un contenu exclusivement numérique peut être renvoyé au néant en quelques clics. Les juges parisiens procèdent donc à un renversement dangereux, en interprétant une abstention latente comme une action sans cesse renouvelée. Présentant un vice de fond, le raisonnement de la Cour d'appel de Paris était de surcroît peu convaincant sur le plan de l'opportunité, puisqu'il aurait autorisé des poursuites pénales antérieurement limitées à trois mois durant des années voire des décennies pour certains contenus. Aussi faut-il se féliciter que d'autres juridictions aient décidé, à l'inverse, qu'il convenait d'appliquer au numérique les mêmes solutions qu'au papier : seule comptait la première publication, le maintien en ligne du message étant indifférent⁴⁸⁴.

Mais le législateur décida, en 2004, de se saisir de la question, et d'y apporter une réponse proche de celle des juges parisiens. Deux situations étaient distinguées par le texte : lorsqu'une publication avait lieu à l'identique sur un support « papier » et sur un support « informatique », les règles habituelles de la loi de 1881 étaient applicables ; en revanche, dès lors que le support était exclusivement numérique, le point de départ de la prescription était repoussé à la date à laquelle le message cessait d'être mis à disposition du public⁴⁸⁵. Saisi avant promulgation de la loi, le Conseil constitutionnel eut à se prononcer sur cette disposition. Aux requérants, qui lui demandaient de condamner une rupture d'égalité devant la loi, il répondit par une formule récurrente en jurisprudence constitutionnelle, selon laquelle « le principe d'égalité ne fait pas obstacle à ce qu'à des situations différentes soient appliquées des règles différentes, dès lors que cette différence de traitement est en rapport direct avec la finalité de la loi qui l'établit »⁴⁸⁶. Il ajouta cependant :

Considérant que, par elle-même, la prise en compte de différences dans les conditions d'accessibilité d'un message dans le temps, selon qu'il est publié sur un support papier ou qu'il est disponible sur un support informatique, n'est pas contraire au principe d'égalité ; que, toutefois, la différence de régime instaurée, en matière de droit de réponse et de prescription, par les dispositions critiquées dépasse manifestement ce qui serait nécessaire pour prendre en compte la situation particulière des messages exclusivement disponibles sur un support informatique [...]»⁴⁸⁷.

Le principe même d'un régime de prescription propre au support numérique n'était donc pas repoussé. Mais les modalités précises choisies par le législateur — un recul potentiellement indéfini

484. - TGI Paris, réf., 30 avr. 1997: *D.*, 1998, somm., 79, obs. J.-Y. Dupeux. V. cep. une décision contraire rendue par la même juridiction le 6 déc. 2000.

485. - Art. 6, V de la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique, dont nous allons voir qu'il a été censuré par le Conseil constitutionnel.

486. - Décision n° 2004-496 DC du 10 juin 2004, considérant n° 13.

487. - *Ibid.*, considérant n° 14.

du départ de la prescription — conduisaient à des résultats excessifs. Une autre possibilité existait : ne rien changer au point de départ, mais modifier la durée de la prescription.

149. Un délai spécial pour les supports numériques ? - En marge de sa théorie de la publication perpétuellement renouvelée, la Cour d'appel de Paris opposait les messages à support écrit ou audiovisuel, qu'elle qualifiait de « périssables, voire furtifs » à ceux publiés sur Internet, supposés plus durables⁴⁸⁸. Si l'on comprend bien, les paroles s'envolent, les écrits sur support papier se putréfient, les écrits électroniques sont (potentiellement) éternels. Dans un rapport sénatorial consacré à *L'équilibre de la loi du 29 juillet 1881 à l'épreuve d'Internet*, une « pérennisation des discours » électroniques dans l'espace public était également dénoncée⁴⁸⁹. « Les technologies de l'Internet accroissent non seulement la persistance des contenus dans l'espace public, mais surtout facilitent leur accessibilité », écrivaient les sénateurs. Ils citaient notamment comme facteurs d'explication les algorithmes utilisés par les réseaux sociaux, qui « mettent en lumière » les messages à succès, et l'indexation des publications par les moteurs de recherche. Si ces phénomènes sont indéniables, n'appellent-ils pas davantage une régulation des plateformes — qui sera abordée plus loin⁴⁹⁰ — qu'un délai allongé de poursuite des auteurs et éditeurs ? Toujours est-il que la proposition numéro 7 du rapport suivait : « Allonger le délai de prescription à un an pour les délits de diffamation, d'injures et de provocation à la discrimination, commis sur Internet ». Peu de temps après le dépôt de ce rapport, ses signataires vinrent arriver devant la Haute assemblée une loi de réforme de la prescription pénale⁴⁹¹. L'un deux déposa un amendement qui distinguait, comme la loi pour la confiance dans l'économie numérique l'avait fait, les publications simultanées sur papier et support électronique, dont le régime restait inchangé, et les publications purement numériques, pour lesquelles le délai de prescription était porté à un an⁴⁹². L'amendement fut adopté, et soutenu par le Sénat durant toutes les étapes ultérieures de la navette législative, mais l'Assemblée nationale, quoique ses rangs fussent divisés, se prononça en majorité contre cette solution. Parmi les arguments employés pour la repousser, on trouve celui-ci :

« C'est justement sur Internet qu'il est facile de trouver des atteintes à la personne, des diffamations. Il est donc beaucoup plus facile de porter plainte, alors qu'auparavant,

488. - V.supra, n°148.

489. - F. Pillet et T. Mohamed Soilihi, rapport précité du 6 juillet 2016.

490. - V.infra, n° 155 s.

491. - Loi n° 2017-242 du 27 février 2017 portant réforme de la prescription en matière pénale

492. - Amendement n° 8 rect. quater du 12 octobre 2016 : « Le premier alinéa de l'article 65 de la loi du 29 juillet 1881 sur la liberté de la presse est complété par une phrase ainsi rédigée : "Lorsque les infractions auront été commises par l'intermédiaire d'un service de communication au public en ligne, sauf en cas de reproduction du contenu d'une publication diffusée sur support papier, l'action publique et l'action civile se prescriront par une année révolue, selon les mêmes modalités". »

avec la seule presse papier, on pouvait passer des mois à éplucher toutes les feuilles de chou de France et de Navarre pour essayer d'y détecter des propos diffamants ou des rumeurs – et ce n'était pas possible, on en loupait ! Bref, internet n'est pas un facteur aggravant, comme on l'affirme beaucoup trop souvent ici depuis le début de la législature : c'est au contraire, dans ce cas précis, un facteur facilitant lorsqu'il s'agit de pouvoir porter plainte »⁴⁹³.

L'idée est assez juste. Cette extrême facilité à convoquer toute l'information existant en ligne sur un individu, à l'aide d'un moteur de recherche, a justifié la jurisprudence européenne sur le droit à l'oubli évoquée plus haut⁴⁹⁴. Présentée alors comme un instrument d'agression de la vie privée, elle peut également être employée à des fins défensives, pour traquer les publications malveillantes, le cas échéant à l'aide d'alertes automatiques, dont il n'existe aucun équivalent pour le papier. En somme, ce n'est pas parce que le Conseil constitutionnel autorise la discrimination entre numérique et papier que cette possibilité doit être employée sans raison convaincante, qu'on peine jusqu'ici à discerner. C'est vrai du moins s'agissant du droit régissant la première publication d'un message : les règles applicables aux nouvelles publications ultérieures des mêmes propos peuvent présenter, en ligne, certaines originalités qu'il faut à présent décrire.

2. - La prescription applicable aux publications ultérieures

150. **La « deuxième vie » d'une publication** - La situation des victimes n'est pas le seul paramètre à prendre en compte, lorsqu'il s'agit de définir les règles de prescription de l'action publique. Idéalement, la possibilité d'engager des poursuites ne devrait prendre fin que si le trouble social suscité par le comportement délictueux a disparu ou s'est suffisamment atténué. Or, si le message potentiellement illicite est ancien, mais qu'il est à nouveau placé en pleine lumière, la blessure infligée aux valeurs de la société peut se raviver. Supposons qu'une telle publication ait eu lieu dans les colonnes d'un premier journal. Si elle est reprise à l'identique, bien plus tard, dans un nouveau numéro, l'infraction sera à nouveau commise, et un nouveau délai de prescription commencera à courir. Quel est l'équivalent numérique d'un tel comportement ? Un autre cas de figure est celui dans lequel la publication initiale n'est pas reprise ni promue par son auteur initial, mais par un tiers. Laissons de côté l'hypothèse d'une mise en avant du contenu par le jeu des algorithmes des plateformes, qui sera envisagée plus loin, et imaginons que c'est une intervention humaine qui donne une seconde vie à un contenu à la fois ancien et illicite. Quelles sont les

493. - Propos de Mme Isabelle Attard, compte-rendu intégral de la première séance de l'Assemblée nationale du 21 janvier 2017.

494. - V.supra, n°104.

conséquences juridiques d'un tel acte ? Autrement dit, alors même que le message initial est resté inchangé, quand peut-on considérer qu'il a été publié une nouvelle fois⁴⁹⁵ ?

Une question du même ordre, quoique plus précise, a été soumise à la Cour de cassation, sous la forme d'une demande d'avis : « L'insertion, dans un article mis en ligne sur Internet, d'un lien hypertexte permettant d'accéder directement à un contenu déjà diffusé, constitue-t-elle un nouvel acte de publication du texte initial faisant à nouveau courir le délai de la prescription trimestrielle prévu par l'article 65 de la loi du 29 juillet 1881 ? »⁴⁹⁶. La Haute juridiction a affirmé ne pas vouloir répondre, aux motifs que :

La demande, qui concerne les conditions dans lesquelles l'insertion dans un article mis en ligne sur le réseau Internet d'un lien hypertexte renvoyant à un texte déjà publié, serait susceptible d'être regardée comme une nouvelle publication de celui-ci, de nature à faire courir à nouveau le délai de prescription de l'article 65 de la loi du 29 juillet 1881 sur la liberté de la presse, suppose un examen des circonstances de l'espèce, notamment de la nature du lien posé et de l'identité de l'auteur de l'article, comme de son intention de mettre à nouveau le document incriminé à la disposition des utilisateurs ; qu'à ce titre, elle échappe à la procédure d'avis prévue par les textes susvisés⁴⁹⁷.

Évidemment, en proposant une liste des éléments de fait qu'il eût été nécessaire de connaître pour conduire un raisonnement juridique, la Cour livre de précieux indices sur les décisions qu'elle rendra par la suite. Parmi ces paramètres dont l'influence lui paraît déterminante, on trouve le fait que le lien a été posté par l'auteur initial du propos ou par un tiers. Il est exact que l'analyse ne peut être conduite à l'identique dans l'un et l'autre cas.

151. Promotion par l'auteur du propos initial - Si elle ne conçoit pas de répondre à une question trop abstraite, la Haute juridiction peut et doit en revanche se prononcer lorsque des pourvois en cassation soumettent à son examen des situations précises. Un plus de deux ans après son refus d'avis, l'occasion lui en fut donnée. Un homme s'était estimé diffamé par l'auteur d'un blog. L'auteur du site avait évoqué un fait attentatoire à l'honneur à deux reprises : dans un premier article suffisamment ancien pour que la prescription soit acquise ; dans un second article, qui

495. - Lorsque le message est modifié, l'analyse est en principe simple : la version amendée est considérée comme une nouvelle publication. Mais là encore, le support numérique n'est pas totalement neutre. L'auteur d'un message qui s'apercevrait, six mois plus tard, qu'il a commis une erreur de ponctuation, ne prendra généralement pas la peine de réaliser une correction si le support initial est le papier. Mais s'il advenait qu'il le fasse tout de même, il l'imprimerait et le distribuerait à nouveau : la seconde publication serait indiscutable. Le même comportement concernant une publication Facebook doit-il être considéré comme une seconde publication ? Sans doute pas si ni le sens du message, ni le public touché par la réapparition éventuelle des propos dans les fils d'actualité des contacts n'en sont modifiés. Si le public a changé, la question mérite d'être posée : V. les développements à suivre.

496. - Avis n° 15008 du 26 mai 2014.

497. - *Ibid.*

renvoyait au premier par le jeu d'un lien hypertexte. La pose de ce lien constituait-elle une nouvelle publication ? La Cour livre une réponse positive qui dépasse largement le cas d'espèce, et frappe par sa large portée :

*Vu l'article 65 de la loi du 29 juillet 1881 ; Attendu qu'il résulte dudit article qu'en matière d'infractions à la loi sur la liberté de la presse, le point de départ de la prescription est le jour de la publication de l'écrit incriminé, par laquelle se consomment les délits que celui-ci peut contenir ; qu'il suit de là que toute reproduction, dans un écrit rendu public, d'un texte déjà publié, est constitutive d'une publication nouvelle dudit texte, qui fait courir un nouveau délai de prescription ; que l'insertion, sur Internet, par l'auteur d'un écrit, d'un lien hypertexte renvoyant directement audit écrit, précédemment publié, caractérise une telle reproduction [...]*⁴⁹⁸.

Au premier abord, la décision semble contraire au raisonnement qu'avait mené la Cour suprême du Canada, à savoir : la création d'un lien hypertexte vers un contenu n'équivaut pas à sa reproduction⁴⁹⁹. Mais, dans l'affaire canadienne, le lien était posé par un tiers vers un contenu dont il n'était pas l'auteur. Dans un tel contexte, nous avons vu que le lien devait en principe être traité comme une « note de bas de page » neutre, à moins qu'il ait été accompagné d'un commentaire matérialisant une approbation ou une adhésion, ou que l'usage d'une technique de lien spécifique aboutisse à en opérer reproduction au sein même de la page Internet du tiers. Dans l'affaire ici soumise à la Cour de cassation, l'auteur du lien était l'auteur du propos initial, et c'est à la lumière de cette circonstance que sa décision doit être comprise. La Cour n'écrit pas que l'insertion d'un lien vaut, de manière générale, reproduction du contenu visé. Cela n'est vrai que lorsqu'il y a identité d'auteur. Il est alors possible de concilier les approches française et canadienne en considérant qu'il s'agit d'une troisième manière de briser la neutralité de principe des liens hypertextes. Et de fait, lorsqu'un auteur renvoie ses lecteurs vers ses propres travaux, il se trouve nécessairement dans une attitude de promotion plutôt que de référencement neutre⁵⁰⁰.

Mais il existe un risque de traiter plus sévèrement le numérique que les supports traditionnels. En effet, comme le relève un auteur, la Cour de cassation distingue en matière de papier entre « nouvelle publication », qui fait courir un nouveau délai de prescription, et la simple « nouvelle diffusion », qui ne permet pas de revenir sur l'écoulement du temps⁵⁰¹. Ainsi, lorsqu'un tract ou un

498. - Cass. crim., 2 nov. 2016, n° 15-87.163 : AJ Pénal, 2017, p. 39, obs. J.-B. Thierry ; D., 2017, p. 203, note A. Serinet ; D. actu., 17 nov. 2016, obs. S. Lavric ; D., 2017, p. 181, n° 24, obs. E. Dreyer.

499. - V.supra, n°137.

500. - *Contra* E. Dreyer, obs. préc. : « [...] ici, c'est la personne qui a réalisé la mise en ligne initiale qui a renvoyé de nouveau vers le contenu litigieux dans le cadre d'un nouvel article accompagné du lien fonctionnant comme un renvoi à ce qui a été précédemment écrit. Cela doit-il modifier l'analyse ? Pas nécessairement : à l'occasion de tout pointage, la volonté d'attirer l'attention du public sur une imputation diffamatoire semble établie ».

501. - La différence de traitement est soulignée par J.-B. Thierry, obs. préc. sur Cass. crim., 2 nov. 2016.

livre a été imprimé en grande quantité, mais que ce stock est distribué en plusieurs fois, seule la première « diffusion » vaut publication⁵⁰². À bien y réfléchir, on ne voit pas pourquoi ressortir un tract des cartons d'un parti politique et le distribuer dans la rue devrait être considéré comme un acte anodin, tandis que la pose d'un lien hypertexte interne à un blog aurait de lourdes conséquences. Le critère tiré de ce qu'il n'a pas été nécessaire de réimprimer le tract paraît absurde — on ne voit pas que la nuisance du document varie selon qu'il est sort d'un tiroir ou d'une photocopieuse -, et il n'est pas transposable au numérique - les documents n'y sortent jamais d'un stock préexistant, et ne bénéficieront jamais de cette étrange exception.

Il est vrai qu'à la fin de sa décision relative au lien hypertexte, la Cour de cassation semble proposer un autre critère modérateur, sans l'avoir fait figurer pourtant dans son attendu de principe. Pour reprocher à la cour d'appel d'avoir admis la prescription, la Cour écrit :

*[...] en statuant ainsi, alors que le texte incriminé avait été rendu à nouveau accessible par son auteur au moyen d'un lien hypertexte, y renvoyant directement, **inséré dans un contexte éditorial nouveau**, la cour d'appel a méconnu le texte susvisé et le principe ci-dessus énoncé [...]*⁵⁰³.

La notion de « contexte éditorial nouveau » est particulièrement fuyante⁵⁰⁴. S'inspirant d'un critère utilisé en droit de la propriété intellectuelle, un auteur propose d'y voir la volonté « d'atteindre un nouveau public », distinct de celui de la première publication⁵⁰⁵. Ne serait-il pas préférable, alors, d'utiliser également ce critère du public nouveau en matière de rediffusion d'un support papier ? N'est-ce pas cela qui devrait justifier une nouvelle possibilité d'exercer des poursuites pénales, lorsqu'un tract est diffusé, plutôt que de se demander si l'encre imbibant le papier était fraîche ou sèche ? Souvent, l'irruption du numérique amène moins à poser des questions nouvelles qu'à poser mieux des questions jusqu'alors mal formulées.

152. Promotion par un tiers - Ici, l'auteur initial du propos illicite n'est pas en cause. Il s'agit de déterminer si une tierce personne peut être considérée comme un nouveau publiant, et donc comme un nouveau contrevenant, par exemple parce qu'elle aurait créé un lien hypertexte vers le

502. - V. not. Cass. crim., 28 oct. 2014, n° 13-86.303 : « [...] la rediffusion d'un même écrit, sans reproduction ni réimpression, ne constitue pas une nouvelle publication [...] ».

503. - *Ibid.* Souligné par nous.

504. - En ce sens : J.-B. Thierry, obs. préc. sur Cass. crim., 2 nov. 2016 ; A. Serinet, note sous le même arrêt. Le critère est encore plus difficile à cerner que celui mentionné dans l'avis de 2014 — et dont on ne trouve plus trace — de « l'intention de mettre à nouveau le document incriminé à la disposition des utilisateurs ».

505. - A. Serinet, note préc. sous Cass. crim., 2 nov. 2016, qui propose un rapprochement avec CJUE, 4e ch., 13 févr. 2014, aff. C-466/12. Sur cette jurisprudence, V.infra, n°217.

contenu initial, ou qu'elle aurait utilisé une fonction de partage d'un réseau social pour le répercuter à ses contacts. Ces questions ont déjà été abordées⁵⁰⁶.

B - L'abondance de contenus illicites

153. Le rôle du ministère public - Les limites assignées à la liberté d'expression sont destinées, le plus souvent, à rester purement virtuelles. Elles sont franchies sans qu'aucune conséquence ne s'abatte sur celui qui a défié la loi française. Une fois encore, le phénomène décrit est ancien dans son principe, mais nouveau dans son intensité. Bien sûr, les propos injurieux, diffamatoires et même racistes, homophobes ou négationnistes se comptent par dizaines de milliers chaque jour dans les bars, les cours de récréation et les rues, sans donner lieu à aucune poursuite. Mais sur Internet, leur caractère écrit et parfois largement public leur confère une violence particulière. Les agresseurs y chassent régulièrement en bandes : des dizaines d'individus s'en prennent tous ensemble à une même cause, à une même catégorie de la population, voire à une même personne. Toutes ces raisons semblent militer pour une répression sévère et aussi systématique que possible.

Malheureusement, des obstacles se présentent alors. Le nombre très important d'infractions est le premier et le plus considérable : les forces de police et de justice s'épuiserait à vouloir les traiter toutes, et n'y parviendraient pas. Le fréquent anonymat derrière lequel se réfugient les internautes constitue un facteur aggravant. Il peut certes être levé, mais au prix d'efforts considérables. Pour sanctionner un simple particulier s'exprimant sur un réseau social, il faut obtenir d'un juge qu'il ordonne à la plateforme de livrer l'adresse IP de l'individu⁵⁰⁷. Puis il faut contraindre le fournisseur d'accès à Internet à révéler l'identité de l'abonné qui utilisait cette adresse IP au moment de la publication. L'accomplissement de ces diverses formalités requiert du temps, des efforts et de l'argent. Les victimes les plus pugnaces, les mieux accompagnées et les mieux organisées ne se laisseront pas arrêter par ces difficultés, et provoqueront au besoin la mise en mouvement de l'action publique en se constituant parties civiles. Restent les autres et, surtout, la défense de l'intérêt général, par la mise en œuvre d'une politique pénale claire et cohérente. Ce n'est pas parce que le ministère public ne peut être partout qu'il est autorisé à n'apparaître nulle part. Il doit choisir ses combats, en fonction de priorités élaborées au niveau national⁵⁰⁸.

506. - V.supra, n°135.

507. - V. par ex. TGI Paris, ordonnance de référé du 24 janvier 2013, *UEJF contre Twitter*. Sur ce qu'est l'adresse IP, V.supra, n°51.

508. - Le ministère public français a le choix de poursuivre ou non les infractions qui lui semblent constituées : article 40-1 du Code de procédure pénale.

154. **L'exemple britannique** - L'adoption d'une politique pénale n'est pas uniquement un moyen d'allouer une ressource rare — en l'espèce, les moyens de police et de justice — en considération de valeurs sociales dont la défense est considérée comme prioritaire. Elle est aussi l'occasion de communiquer sur ces priorités auprès du grand public, afin de dissuader les potentiels auteurs d'infraction, en leur donnant un aperçu de la rigueur avec laquelle ils seraient traités s'ils se laissaient aller à adopter certains comportements. Ainsi le *Crown Prosecution Service* (CPS) britannique a-t-il donné une large publicité à ses *Guidelines on prosecuting cases involving communications sent via social media*⁵⁰⁹. La première version, adoptée en 2013, détaillait les affaires qui devaient faire prioritairement l'objet de poursuites publiques, en particulier les menaces crédibles de violence contre les biens ou les personnes, harcèlement, propos violemment offensants⁵¹⁰. En 2016, une nouvelle version du document a été adoptée. Elle promet par exemple de s'attaquer aux organisateurs de campagnes de harcèlement collectif sur les réseaux⁵¹¹. Ainsi, le CPS s'est doté d'une doctrine précise, il l'a médiatisée et l'a déjà révisée pour tenir compte de l'apparition ou de l'inflation de certaines pratiques en ligne qui outrepassent les limites de la liberté d'expression. Ajoutons que le CPS propose aux internautes d'alimenter ses réflexions sur ses sujets, en lançant de vastes campagnes de consultations⁵¹².

La France ne semble pas avoir adopté jusqu'ici de stratégie publique de lutte contre les abus de la liberté d'expression en ligne. Avant d'envisager de toucher au fond du droit, et de doter l'expression numérique de règles qui lui seraient spéciales, sans doute faudrait-il concevoir et appliquer une politique pénale propre à lui appliquer sérieusement l'arsenal juridique existant : on pourrait bien s'apercevoir, alors, que cela est suffisant. Encore faudra-t-il accompagner cette stratégie dirigée vers les auteurs d'une réflexion visant à affiner le statut des plateformes, ces intermédiaires qui livrent et mettent en scène l'information produite par d'autres.

509. - http://www.cps.gov.uk/legal/a_to_c/communications_sent_via_social_media/.

510. - Version du 20 juin 2013.

511. - Le communiqué accompagnant la révision du document indique ainsi : « *The new social media guidelines for prosecutors make clear that those who encourage others to participate in online harassment campaigns - known as 'virtual mobbing' - can face charges of encouraging an offence under the Serious Crime Act 2007* » (

« CPS publishes new social media guidance and launches Hate Crime consultation », article du 10/10/16 sur cps.gov.uk.

512. - <http://www.cps.gov.uk/consultations/>.

Section 2 - La canalisation de l'information

155. **Des éditeurs aux plateformes : une évaporation de la responsabilité** - La situation des producteurs d'information — ceux qui parlent, ceux qui écrivent, ceux qui font un usage direct et personnel de la liberté d'expression — ne semblait pas rendre indispensable l'émergence d'un droit nouveau propre au numérique. Le support électronique ne faisait que poser des questions préexistantes avec une intensité, sous des angles et dans des contextes nouveaux. Cela rend certes nécessaire un travail doctrinal et jurisprudentiel d'adaptation des concepts anciens — des pistes ont été proposées -, mais pas davantage.

La situation des intermédiaires de la communication numérique est tout autre. On peine à identifier un strict équivalent de ces acteurs à l'ère précédente, celle du papier. Sans ces hébergeurs, ces réseaux sociaux, mais aussi ces moteurs de recherche, la « conversation mondiale sans fin » n'aurait pas lieu⁵¹³. Pourtant, leur rôle n'a rien de comparable avec celui d'un éditeur de publication sur papier ; les règles qui leur sont applicables ne peuvent par conséquent pas être les mêmes.

Le droit de la presse connaît, sous l'empire de la loi de 1881, un régime de responsabilité dit « en cascade » : une infraction de presse est réputée commise en priorité par « Les directeurs de publications ou éditeurs, quelles que soient leurs professions ou leurs dénominations [...] » . Ce n'est qu'à défaut de pouvoir les poursuivre qu'on s'en prendra aux auteurs ou, à défaut d'auteur, aux imprimeurs, et enfin en dernier recours aux « imprimeurs, vendeurs, distributeurs et afficheurs »⁵¹⁴. Ce n'est donc pas l'auteur, dans un tel système, qui occupe le premier rang, mais bien les directeurs de publication ou éditeurs, c'est-à-dire des individus qui n'ont pas conçu les propos incriminés. D'autres les ont imaginés et les leur ont soumis ; eux ont pris la décision de les assumer de telle sorte que, si la justice devait demander compte de leur légalité, elle s'en prendrait à eux comme auteurs principaux du délit.

Ce modèle est encore transposable à une partie de la circulation d'information en ligne. De nombreux sites Internet ont la maîtrise de leur contenu : ils ne constituent pas des simples intermédiaires par lesquels transiteraient les propos des autres. Cette situation concerne aussi bien les sites de grands journaux que les simples blogs de particuliers. Dans ces situations, un directeur de publication doit encore être nommé, et une responsabilité en cascade, conçue d'une manière légèrement différente, est prévue par la loi⁵¹⁵. Mais même sur de tels sites, il est fréquent de trouver

513. - V. supra, n° 118.

514. - Art. 42 de la loi de 1881 précitée.

515. - Art. 93-3 al. 1 à 3 de la loi n° 82-652 du 29 juillet 1982 sur la communication audiovisuelle.

un espace permettant à leurs visiteurs de proposer leurs commentaires sur les contenus affichés. Ces commentaires ne font pas toujours l'objet d'une modération *a priori*. Cohabitent alors deux espaces : l'un dont le contenu est entièrement au pouvoir de l'éditeur, l'autre qui échappe largement à son contrôle, au moins provisoirement. Cette nature hybride appelle un régime juridique différencié.

La logique d'absence de contrôle préalable des contenus est portée à son paroxysme dans le cas des hébergeurs, des réseaux sociaux, ou dans celui des moteurs de recherche. L'espace éditorial propre n'y existe pas, et subsiste un pur support, un ensemble de tuyaux par lesquels se précipitent des cascades d'information, dans des volumes qui découragent toute velléité de contrôle humain, systématique et *a priori*. On avance le chiffre de 30 000 milliards de pages indexées par Google, et de 500 millions de tweets envoyés chaque jour⁵¹⁶.

À contempler ces chiffres, il semble évident que les obligations pesant sur ces intermédiaires et la responsabilité qu'ils doivent encourir ne peuvent avoir la même intensité que celles qui incombent au directeur d'une publication. Les revendications de ces nouveaux acteurs vont évidemment en ce sens. Puisqu'il semble impossible de contrôler ce que charrie le torrent d'information, puisque leur office est essentiellement technique et en aucun cas intellectuel, elles devraient être juridiquement translucides. Ce phénomène d'effacement et de responsabilisation des intermédiaires se retrouvera d'ailleurs lorsque seront envisagées les plateformes visant non plus à la communication, mais à la rencontre entre une offre et une demande de services. Les mêmes logiques y sont à l'œuvre.

156. Une nécessaire régulation - Cette présentation des plateformes comme impuissantes à vérifier quels contenus transitent par leur intermédiaire est à nuancer, et le réalisme ne doit pas se muer en cynisme. Plusieurs raisons militent en faveur d'un contrôle sérieux de ces intermédiaires. D'abord, s'il leur est impossible d'exercer un contrôle systématique et *a priori* des publications, il est parfois envisageable de leur demander un contrôle *a posteriori*, sur la base de signalements, et visant au retrait des contenus manifestement illicites (I). Ensuite, il est possible de s'intéresser à la manière dont ces intermédiaires agencent l'information. S'ils n'assurent évidemment pas un travail de rédaction en chef auprès des internautes, ils ne se contentent pas non plus d'ouvrir le robinet des contenus sans aucun égard pour ce qui transiterait dans leurs tuyaux. La matière brute doit être retravaillée, fût-ce au moyen d'algorithmes, afin qu'elle ait quelque intérêt pour les internautes qui consultent les plateformes, et pour les publicitaires qui les rémunèrent. Ces algorithmes trient, hiérarchisent, agencent les publications, leur confèrent une visibilité moindre ou supérieure par

516. - Chiffres proposés par *blogdumoderateur.com* (actualisés au 23 novembre 2016).

rapport à ce qui aurait été le résultat d'une formule concurrente ou d'un simple tri chronologique. La question de l'encadrement de cette activité peut être posée (II).

I - La suppression de l'information

157. **Deux catégories d'intermédiaires** - Il faut ici distinguer deux types d'acteurs. Les FAI, d'abord, offrent à leurs abonnés une porte d'entrée dans le réseau. À ce titre, ils transportent des données entre une multitude d'utilisateurs et de services sans lien les uns avec les autres. Les hébergeurs, ensuite, assurent un service précis de stockage, et parfois de mise en forme automatisée, des contenus fournis par leurs utilisateurs. Chacune de ces catégories d'opérateurs entretient donc un rapport distancié avec les publications finales, dont ils ne sont que les véhicules. Leur degré de passivité diffère toutefois. Il est plus élevé chez le FAI, qui gère les « tuyaux » à travers lesquels transitera toute l'information du monde. Il est moindre chez l'hébergeur, maître d'un service aux contours définis : il n'a certes pas une connaissance *a priori* des contenus publiés à l'aide de ses bons offices ; mais il n'a qu'un effort limité à accomplir s'il veut savoir. Ce rôle passif qu'ils ont en partage, cette communauté partielle de nature, appelle l'existence d'obligations communes aux deux catégories. Mais la nette différence de degré qui vient d'être exposée justifie par ailleurs l'existence de règles qui leur sont propres.

158. **Règles communes** - Ni les FAI, ni les hébergeurs ne sont soumis « à une obligation générale de surveiller les informations qu'[ils] transmettent ou stockent, ni à une obligation générale de rechercher des faits ou des circonstances révélant des activités illicites »⁵¹⁷. S'il leur fallait opérer un contrôle *a priori* des montagnes de données qui transitent par leurs services, par crainte d'être personnellement tenu responsable d'un défaut général de vigilance, la tâche serait écrasante.

Toutefois, le législateur apporte à cette position de principe un certain nombre de tempéraments. Il précise ainsi que l'autorité judiciaire est en droit de leur demander de procéder à des actions « de surveillance ciblée et temporaire »⁵¹⁸.

Il estime aussi et surtout que « compte de l'intérêt général attaché à la répression » de certaines infractions particulièrement odieuses, qui sont énumérées ils doivent « concourir » à lutter contre elles⁵¹⁹. Quelles formes concrètes cette lutte doit-elle emprunter ? Il leur faut avant tout proposer à

517. - Loi n° 2004-575 précitée, art. 6, I, 7.

518. - *Loc. cit.*

519. - « Compte tenu de l'intérêt général attaché à la répression de l'apologie des crimes contre l'humanité, de la provocation à la commission d'actes de terrorisme et de leur apologie, de l'incitation à la haine raciale, à la haine à l'égard de personnes à raison de leur sexe, de leur orientation ou identité sexuelle ou de leur handicap ainsi que de la pornographie infantile, de l'incitation à la violence, notamment l'incitation aux violences faites aux

leurs utilisateurs un dispositif de signalement facile d'accès, permettant de porter à leur connaissance l'illicéité manifeste qu'ils auraient repérée⁵²⁰. La surveillance générale et automatique « par le haut » étant impossible, elle est remplacée par une surveillance humaine et au cas par cas, « par le bas ». Ce signalement opéré, les faits qui en sont à l'origine doivent être vérifiés par les services du professionnel. Si l'illicéité est confirmée par cet examen, aussi bien les FAI que les hébergeurs ont l'obligation de prendre « promptement » attache avec les autorités publiques compétentes⁵²¹. On relèvera que la loi prévoit, dans un alinéa spécifiquement dédié, un dispositif de signalement et de révélation aux autorités fonctionnant sur le même principe que celui qui vient d'être décrit, mais spécifique aux jeux d'argent illégaux en ligne⁵²². Il pourrait s'agir de l'amorce d'une législation par énumération, dont la lecture serait malaisée et les priorités indécélables.

La loi consacre encore, à la charge des FAI aussi bien que des hébergeurs, une obligation de « rendre publics les moyens qu'[ils] consacrent à la lutte contre ces activités illicites »⁵²³. Il n'est pas certain qu'elle soit scrupuleusement respectée⁵²⁴. Au fond, est-ce important ? L'essentiel n'est pas que les moyens soient rendus publics, mais qu'ils soient suffisants, ce que seuls des tests réalisés par une administration publique permettraient de révéler. De telles études de terrain officielles ont été conduites en Allemagne⁵²⁵.

Il est affirmé par ailleurs : « L'autorité judiciaire peut prescrire en référé ou sur requête, à toute personne mentionnée au 2 [les hébergeurs] ou, à défaut, à toute personne mentionnée au 1 [les FAI], toutes mesures propres à prévenir un dommage ou à faire cesser un dommage occasionné par le contenu d'un service de communication au public en ligne »⁵²⁶. L'intérêt de ce texte, par rapport au droit commun des référés par exemple, est qu'il pose une hiérarchie entre les destinataires. L'ordre

femmes, ainsi que des atteintes à la dignité humaine, les personnes mentionnées ci-dessus doivent concourir à la lutte contre la diffusion des infractions visées aux cinquième, septième et huitième alinéas de l'article 24 de la loi du 29 juillet 1881 sur la liberté de la presse et aux articles 225-4-1, 225-5, 225-6, 227-23 et 227-24 et 421-2-5 du code pénal » (*Loc. cit.*).

520. - *Loc. cit.*

521. - *Loc. cit.*

522. - *Loc. cit.* : « Compte tenu de l'intérêt général attaché à la répression des activités illégales de jeux d'argent, les personnes mentionnées aux 1 et 2 mettent en place, dans des conditions fixées par décret, un dispositif facilement accessible et visible permettant de signaler à leurs abonnés les services de communication au public en ligne tenus pour répréhensibles par les autorités publiques compétentes en la matière. Elles informent également leurs abonnés des risques encourus par eux du fait d'actes de jeux réalisés en violation de la loi ».

523. - *Loc. cit.* À supposer qu'elle soit respectée, du reste, cette obligation a-t-elle un intérêt véritable ?

524. - Une recherche dans un moteur sur l'expression « moyens de lutte contre les activités illicites » associée au nom d'un fournisseur d'accès ne renvoie guère de résultat probant.

525. - *V.infra*, n°162.

526. - Loi n° 2004-575 précite, art. 6, I, 8.

doit être donné par préférence aux hébergeurs et, seulement lorsque cela n'est pas possible, aux FAI⁵²⁷.

159. La remise en cause de l'obligation commune de conservation des données - Enfin, il est imposé aux FAI et hébergeurs de conserver « les données de nature à permettre l'identification de quiconque a contribué à la création du contenu ou de l'un des contenus des services dont elles sont prestataires »⁵²⁸. Comme il a été longuement démontré, les producteurs d'information ont théoriquement à répondre, plus que les intermédiaires, de leurs publications illicites⁵²⁹. Encore faut-il être en mesure d'imputer une éventuelle infraction pénale ou faute civile au bon individu, sans s'arrêter à l'apparence trompeuse qui peut résulter de l'usage d'un pseudonyme, ou de celui d'un nom véritable usurpé. La conservation exhaustive des adresses IP, reliées à l'historique des actions effectuées en ligne par l'abonné correspondant, sert à l'évidence un tel objectif. Mais une telle pratique n'est pas sans risque pour la vie privée des individus, en ce qu'elle crée un réservoir de données sensibles : qui parle à qui, combien de temps, qui professe tel discours en ligne, qui consulte telle information sur Internet. Le risque existe que cette manne soit exploitée au-delà du strict nécessaire à la lutte contre la délinquance. La Cour de justice de l'Union européenne a rendu deux arrêts qui traitent précisément de ces questions.

Le premier arrêt, connu sous le nom de *Digital Rights Ireland*, date de 2014⁵³⁰. Il était question de la compatibilité d'une directive de 2006, qui constituait la source européenne de cette obligation de conservation des données, avec la Charte des droits fondamentaux⁵³¹. La Cour affirme d'abord que cette obligation constitue une ingérence dans le droit au respect de la vie privée et à la protection des données à caractère personnel⁵³². Une telle ingérence est possible lorsqu'elle répond à un objectif d'intérêt général, et qu'elle est proportionnée. Poursuivent bien un intérêt général des dispositions qui visent « à garantir la disponibilité de ces données à des fins de recherche, de détection et de poursuite d'infractions graves telles qu'elles sont définies par chaque État membre dans son droit interne. L'objectif matériel de cette directive est, dès lors, de contribuer à la lutte

527. - V.infra, n°166.

528. - Loi n° 2004-575 précitée, art. 6, II.

529. - V.supra, n°123.

530. - CJUE, 8 avril 2014, C-293/12 et C-594/12, *Digital Rights Ireland Ltd c./ Minister for Communications, Marine and Natural Resources*.

531. - Directive 2006/24/CE du Parlement européen et du Conseil du 15 mars 2006 sur la conservation de données générées ou traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public ou de réseaux publics de communications, et modifiant la directive 2002/58/CE (directive vie privée et communications électroniques).

532. - §34 et suivants.

contre la criminalité grave et ainsi, en fin de compte, à la sécurité publique »⁵³³. Restait à savoir si l'atteinte aux droits fondamentaux était proportionnée. Or, la Cour relève notamment que :

*[...] la directive 2006/24 concerne de manière globale l'ensemble des personnes faisant usage de services de communications électroniques, sans toutefois que les personnes dont les données sont conservées se trouvent, même indirectement, dans une situation susceptible de donner lieu à des poursuites pénales. Elle s'applique donc même à des personnes pour lesquelles il n'existe aucun indice de nature à laisser croire que leur comportement puisse avoir un lien, même indirect ou lointain, avec des infractions graves. En outre, elle ne prévoit aucune exception, de sorte qu'elle s'applique même à des personnes dont les communications sont soumises, selon les règles du droit national, au secret professionnel*⁵³⁴.

*[...] la directive 2006/24 ne prévoit aucun critère objectif permettant de limiter le nombre de personnes disposant de l'autorisation d'accès et d'utilisation ultérieure des données conservées au strict nécessaire au regard de l'objectif poursuivi. Surtout, l'accès aux données conservées par les autorités nationales compétentes n'est pas subordonné à un contrôle préalable effectué soit par une juridiction, soit par une entité administrative indépendante dont la décision vise à limiter l'accès aux données et leur utilisation à ce qui est strictement nécessaire [...]*⁵³⁵.

*[...] s'agissant de la durée de conservation des données, la directive 2006/24 impose, à son article 6, la conservation de celles-ci pendant une période d'au moins six mois sans que soit opérée une quelconque distinction entre les catégories de données prévues à l'article 5 de cette directive en fonction de leur utilité éventuelle aux fins de l'objectif poursuivi ou selon les personnes concernées*⁵³⁶.

À la suite de cet arrêt, deux questions principales étaient posées⁵³⁷. La première : une obligation de conservation des données qui conserverait un caractère général était-elle encore envisageable, à supposer qu'elle soit mieux encadrée du point de vue des délais de conservation, de la qualité des personnes autorisées à consulter les registres, de l'existence d'un contrôle administratif ou judiciaire ? On pouvait le croire. La deuxième question : les dispositions nationales pouvaient-elles survivre à l'invalidation de la directive ? En effet, « conformément à l'article 51 § 1 de la Charte, les dispositions de cette dernière sont applicables aux États membres uniquement lorsqu'ils mettent en œuvre le droit de l'Union, c'est-à-dire, selon la jurisprudence de la Cour, lorsqu'une réglementation nationale entre dans le champ d'application du droit de l'Union. Or, du fait de l'invalidité rétroactive de la directive n° 2006/24/CE, il n'était pas évident que les dispositions nationales qui prévoyaient la conservation des données de connexion aux fins de leur mise à

533. - §41.

534. - §58.

535. - §62.

536. - §63.

537. - Sur lesquelles V. not. F.-X. Bréchet, note ss. CJUE, 21 déc. 2016, *Rev. UE*, 2017, 178.

disposition éventuelle des autorités publiques entraient toujours dans le champ d'application du droit de l'Union »⁵³⁸.

Un second arrêt apporte des réponses claires, et prend le parti d'une forte protection de la vie privée des internautes. Rendu à la fin de l'année 2016, il est connu sous le nom de *Tele2 Sverige AB*⁵³⁹. La Cour écrit d'abord que les réglementations nationales sur la conservation des données de connexion entrent bien dans le champ des directives⁵⁴⁰. Il n'est donc plus possible d'affirmer qu'elles peuvent subsister sans le support du droit de l'Union, qui constitue tout au contraire leur nécessaire soubassement. C'est ensuite et surtout le principe même d'une conservation indifférenciée de l'ensemble des données relatives au trafic sur Internet qui est condamné. En effet, pour qu'une réglementation nationale soit valable :

*Elle doit en particulier indiquer en quelles circonstances et sous quelles conditions une mesure de conservation des données peut, à titre préventif, être prise, garantissant ainsi qu'une telle mesure soit limitée au strict nécessaire*⁵⁴¹.

*S'agissant de la délimitation d'une telle mesure quant au public et aux situations potentiellement concernés, la réglementation nationale doit être fondée sur des éléments objectifs permettant de viser un public dont les données sont susceptibles de révéler un lien, au moins indirect, avec des actes de criminalité grave, de contribuer d'une manière ou d'une autre à la lutte contre la criminalité grave ou de prévenir un risque grave pour la sécurité publique. Une telle délimitation peut être assurée au moyen d'un critère géographique lorsque les autorités nationales compétentes considèrent, sur la base d'éléments objectifs, qu'il existe, dans une ou plusieurs zones géographiques, un risque élevé de préparation ou de commission de tels actes*⁵⁴².

La Cour ajoute ensuite des exigences relatives, notamment, aux conditions d'accès par les autorités aux données ainsi enregistrées⁵⁴³. Mais il s'agit cette fois-ci clairement d'un temps distinct du raisonnement, de sorte qu'un encadrement rigoureux sur ce point ne sauverait pas l'obligation de conservation générale des données, qui a auparavant été condamnée dans son principe même.

Il est donc clair que le droit français sur ce point n'est pas conforme à la jurisprudence de la CJUE, et qu'il devra rapidement évoluer.

Les règles communes aux FAI et aux hébergeurs ayant été présentées, il faut à présent aborder les dispositions spécifiques à chacune de ces deux catégories d'intermédiaires techniques.

538. - F.-X. Bréchet, note préc.

539. - CJUE, 21 décembre 2016, C-203/15, *Tele2 Sverige AB (C-203/15)* : F.-X. Bréchet, note préc.

540. - §81.

541. - §109.

542. - §111.

543. - §118 et s.

160. **Règles spéciales** - Au rôle différent qu'ils assument dans la diffusion des informations en ligne répondent des obligations différentes lorsqu'il s'agit de faire disparaître des contenus manifestement illicites. Les intermédiaires techniques doivent, fréquemment, retirer des publications qui leur ont été signalées (A). Les FAI doivent, dans des cas exceptionnels, organiser l'impossibilité pure et simple d'entrer en contact avec certains sites Internet (B).

A - Le retrait de contenus par les intermédiaires techniques après signalement

161. **Un régime spécial de responsabilité** - Il est difficile d'obtenir une régulation satisfaisante de la liberté d'expression lorsque seuls les producteurs d'information sont punis pour leurs abus. À s'en tenir même aux violations les plus manifestes de la liberté d'expression, le nombre et l'anonymat des auteurs constituent, on l'a dit, autant de freins à des sanctions efficaces⁵⁴⁴. Les intermédiaires, en revanche, sont — relativement — peu nombreux, identifiés, solvables. Il est ainsi plus aisé de faire peser sur eux des obligations en matière de lutte contre les expressions illicites, et de rechercher leur responsabilité civile ou pénale en cas de défaillance. Qui sont-ils, et que peut-on attendre d'eux ? La loi sur la confiance dans l'économie numérique, transposant une directive européenne, apporte une réponse en matière de responsabilité civile⁵⁴⁵.

*Les personnes physiques ou morales qui assurent, même à titre gratuit, pour mise à disposition du public par des services de communication au public en ligne, le stockage de signaux, d'écrits, d'images, de sons ou de messages de toute nature fournis par des destinataires de ces services ne peuvent pas voir leur responsabilité civile engagée du fait des activités ou des informations stockées à la demande d'un destinataire de ces services si elles n'avaient pas effectivement connaissance de leur caractère illicite ou de faits et circonstances faisant apparaître ce caractère ou si, dès le moment où elles en ont eu cette connaissance, elles ont agi promptement pour retirer ces données ou en rendre l'accès impossible*⁵⁴⁶.

L'alinéa suivant du même texte pose de semblables conditions et obstacles à la responsabilité pénale. Une autre loi adopte la même solution s'agissant des sites à contenu hybride : ceux dont une partie ne fait pas l'objet d'un contrôle *a priori*, par exemple un espace de commentaires offert aux lecteurs⁵⁴⁷.

544. - V.supra, n°153.

545. - Il s'agit d'une transposition de l'article 14§1 de la directive 2000/31/CE du Parlement européen et du Conseil du 8 juin 2000 relative à certains aspects juridiques des services de la société de l'information, et notamment du commerce électronique, dans le marché intérieur.

546. - Art. 6, I, 2 de la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique. Sur les difficultés d'interprétation de ce texte, V. not. J. Bossan, « Le droit pénal confronté à la diversité des intermédiaires de l'Internet », *RSC*, 2013, 295 ; F. Chopin, « Cybercriminalité », art. préc., n° 344 s.

547. - Art. 93-3, dernier alinéa de la loi n° 82-652 du 29 juillet 1982 sur la communication audiovisuelle : « Lorsque l'infraction résulte du contenu d'un message adressé par un internaute à un service de communication au public en ligne et mis par ce service à la disposition du public dans un espace de contributions personnelles

Qui sont les personnes visées par ces textes ? Il s'agit de tout intermédiaire qui fait apparaître en ligne des données fournies par des tiers, sans en prendre connaissance au préalable. C'est le cas des sociétés hébergeant les sites Internet conçus par leurs clients, des réseaux sociaux et sites communautaires⁵⁴⁸, de moteurs de recherche⁵⁴⁹ ou encore de plateformes vidéo⁵⁵⁰. Le fait que des algorithmes manipulent les contenus sans intervention humaine, afin d'en assurer la publication, ne suffit pas à ce que l'on considère que ces contenus ont été portés à la connaissance de l'intermédiaire⁵⁵¹. En revanche, dès lors que l'intermédiaire prétendu a assumé un rôle de conseil qui suppose qu'il ait pris connaissance du contenu proposé par le tiers, il perd le bénéfice de ces immunités civiles et pénales⁵⁵².

identifié comme tel, le directeur ou le codirecteur de publication ne peut pas voir sa responsabilité pénale engagée comme auteur principal s'il est établi qu'il n'avait pas effectivement connaissance du message avant sa mise en ligne ou si, dès le moment où il en a eu connaissance, il a agi promptement pour retirer ce message ».

548. - Par ex., à propos du site collaboratif Fuzz : « la cour d'appel qui a relevé que l'activité de la société Bloobox-net, créatrice du site www.fuzz.fr, se bornait à structurer et classer les informations mises à la disposition du public pour faciliter l'usage de son service, mais que cette société n'était pas l'auteur des titres et des liens hypertextes, ne déterminait ni ne vérifiait les contenus du site, en a exactement déduit que relevait du seul régime applicable aux hébergeurs, la responsabilité de ce prestataire, fût-il créateur de son site, qui ne jouait pas un rôle actif de connaissance ou de contrôle des données stockées » (Cass. 1ère civ., 17 févr. 2011, n° 09-13.202).

549. - Ainsi, à propos des moteurs de recherche : la CJUE décide de leur appliquer l'article 14 de la directive 2000/31/CE, que la loi sur la confiance dans l'économie numérique a transposé : « lorsque ce prestataire n'a pas joué un rôle actif de nature à lui confier une connaissance ou un contrôle des données stockées. S'il n'a pas joué un tel rôle, ledit prestataire ne peut être tenu responsable pour les données qu'il a stockées à la demande d'un annonceur à moins que, ayant pris connaissance du caractère illicite de ces données ou d'activités de cet annonceur, il n'ait pas promptement retiré ou rendu inaccessibles lesdites données » (CJUE, *Google France SARL, Google Inc. c. Louis Vuitton Malletier SA*, 23 mars 2010, C236/08).

550. - V. l'ex. de Dailymotion à la note suivante.

551. - À propos de l'hébergeur vidéo Dailymotion, la Cour de cassation approuve des juges du fond d'avoir décidé que « le réencodage de nature à assurer la compatibilité de la vidéo à l'interface de visualisation, de même que le formatage destiné à optimiser la capacité d'intégration du serveur en imposant une limite à la taille des fichiers postés, sont des opérations techniques qui participent de l'essence du prestataire d'hébergement et qui n'induisent en rien une sélection par ce dernier des contenus mis en ligne, que la mise en place de cadres de présentation et la mise à disposition d'outils de classification des contenus sont justifiés par la seule nécessité, encore en cohérence avec la fonction de prestataire technique, de rationaliser l'organisation du service et d'en faciliter l'accès à l'utilisateur sans pour autant lui commander un quelconque choix quant au contenu qu'il entend mettre en ligne ; qu'il ajoute que l'exploitation du site par la commercialisation d'espaces publicitaires n'induit pas une capacité d'action du service sur les contenus mis en ligne ; que de l'ensemble de ces éléments la cour d'appel a exactement déduit que la société Dailymotion était fondée à revendiquer le statut d'intermédiaire technique au sens de l'article 6-I-2 de la loi du 21 juin 2004 » (Cass. 1ère civ., 17 févr. 2011, n° 09-67.896).

552. - La Cour de cassation a approuvé des juges du fond d'avoir relevé « que les sociétés eBay fournissent à l'ensemble des vendeurs des informations pour leur permettre d'optimiser leurs ventes et les assistent dans la définition et la description des objets mis en vente en leur proposant notamment de créer un espace personnalisé de mise en vente ou de bénéficier "d'assistants vendeurs" ; qu'il relève encore que les sociétés eBay envoient des messages spontanés à l'attention des acheteurs pour les inciter à acquérir et invitent l'enchérisseur qui n'a pu remporter une enchère à se reporter sur d'autres objets similaires sélectionnés par elles ; que de ces constatations et appréciations, la cour d'appel a pu déduire que les sociétés eBay n'avaient pas exercé une simple activité d'hébergement, mais qu'elles avaient, indépendamment de toute option choisie par les vendeurs, joué un rôle actif de nature à leur conférer la connaissance ou le contrôle des données qu'elles stockaient et à les priver du régime exonératoire de responsabilité prévu par l'article 6.1.2 de la loi du 21 juin 2004 et l'article 14 §1 de la directive

162. Une efficacité insuffisante en pratique ? - Ces immunités cèdent lorsque les intermédiaires avaient connaissance des contenus soit dès leur publication — un exemple vient d'en être donné — soit postérieurement, parce qu'ils ont été signalés par d'autres utilisateurs comme manifestement illicites et que l'intermédiaire n'a pas réagi « promptement ». Ces dispositions sont-elles d'une sévérité suffisante ? Dans un courrier interne à l'entreprise, mais dont la presse a eu connaissance, le PDG de Twitter reconnaissait que son entreprise avait été « nulle » en matière de prise en compte des signalements, notamment dans la lutte contre le harcèlement en ligne⁵⁵³. De tels propos laissent craindre que les plateformes, lorsqu'elles suivent leur pente naturelle, ne soient pas suffisamment diligentes en la matière. Il reviendrait alors au droit de combattre, par des dispositions sévères, cette coupable inertie. Récemment, le débat public allemand est allé en ce sens. Le droit allemand connaît le même type d'obligations à la charge des intermédiaires de la communication en ligne, puisqu'il a été rappelé qu'elles ont une origine européenne. Le Ministère fédéral de la Famille et le Ministère fédéral de la Justice et de la Protection des consommateurs ont réalisé une série de tests, en signalant à ces opérateurs plusieurs centaines de contenus manifestement illicites et en examinant leur réaction⁵⁵⁴. Si YouTube avait opéré plus de 90% de suppressions, le chiffre n'était plus que de 39% pour Facebook, et de moins de 1% pour Twitter. Du moins s'agissait-il des résultats obtenus lorsqu'un utilisateur ordinaire avait opéré le signalement. Ces chiffres s'amélioraient lorsque c'était un compte « vérifié » qui s'en était chargé — il s'agit d'un compte dont la plateforme a contrôlé l'identité par une prise de contact direct hors-ligne -, et plus encore lorsque le signalement a lieu par courrier électronique⁵⁵⁵. Estimant ces résultats insuffisants, le ministre de la Justice allemand Heiko Maas a mis au point un projet de loi, dont la première version était particulièrement sévère, dans le but affiché de nettoyer les écuries d'Augias. Les contenus manifestement illicites devaient être supprimés dans les 24 heures, et les contenus dont l'illicéité nécessitait un examen plus approfondi, dans les 7 jours⁵⁵⁶. En cas de manquement, une sanction

2000/31 ». Pourtant, les sollicitations décrites peuvent être réalisées par le site de manière parfaitement automatisée, et ce n'est que lorsque le client sollicite un « assistant vendeur » que la société acquiert une connaissance personnelle des données.

553. - <http://www.france24.com/fr/20150205-twitter-est-nul-harcelement-avoue-son-pdg-dick-costello-trolls-lindy-west-anita-sarkeesian/>.

554. - Les résultats sont consultables sur le site du ministère fédéral de la Justice et de la protection des consommateurs : http://www.fair-im-netz.de/SharedDocs/Downloads/DE/Artikel/03142017_Monitoring_jugendschutz.net.pdf?__blob=publicationFile&v=3.

555. - Pour Twitter : 1% de suppression après signalement ordinaire, 63% après un signalement par un compte vérifié, 36 après l'envoi d'un courriel. Pour YouTube, les chiffres sont respectivement de 90%, 7% et 3%. Facebook se distingue en laissant 7% de contenus illicites en ligne même après l'emploi de toutes les méthodes de signalement.

556. - Le texte du projet de loi peut être consulté (en langue allemande) à l'adresse : <http://ec.europa.eu/growth/tools-databases/tris/fr/index.cfm/search/>

personnelle allant jusqu'à 5 millions d'euros pouvait frapper le responsable des signalements au sein de l'entreprise, quand l'amende infligée à la société elle-même était susceptible d'atteindre 50 millions d'euros. À première vue, la France aurait tout intérêt à suivre le même chemin. Et pourtant, les options draconiennes de M. Maas ne sont pas sans danger.

163. Une police privée de la liberté d'expression - La jurisprudence européenne reconnaît aux personnes physiques, dans certains cas, le droit d'obtenir que soient retirés d'un moteur de recherche certains résultats obsolètes, intrusifs et qui ont perdu leur pertinence⁵⁵⁷. Il nous avait semblé inquiétant que les moteurs aient à prendre la décision de première ligne consistant à accepter ou à refuser d'occulter une information - et qu'ils soient même les seuls à connaître du dossier lorsqu'ils donnent une suite favorable à la demande qui leur est présentée.

Le même danger existe, ici, que se constitue une police privée des contenus. Le projet allemand semble excessif, aussi bien dans la substance des obligations qu'il met à la charge des plateformes que dans les sanctions qu'il fulmine pour assurer leur exécution.

D'abord, les obligations envisagées sont dangereuses, en ce qu'elles ne limitent pas le champ d'intervention des intermédiaires à ce qui est manifestement illicite. Moyennant un délai plus long, ces sociétés privées ont vocation à se prononcer, de l'aveu même du projet de loi, sur des situations dans lesquelles la licéité de l'expression visée fait débat. La loi française pour la confiance dans l'économie numérique semble tomber dans le même travers, lorsqu'elle vise le caractère simplement « illicite » des contenus signalés. Bien heureusement, le Conseil constitutionnel a posé une très importante réserve d'interprétation.

*Considérant que les 2 et 3 du I de l'article 6 de la loi déférée ont pour seule portée d'écarter la responsabilité civile et pénale des hébergeurs dans les deux hypothèses qu'ils envisagent ; que ces dispositions ne sauraient avoir pour effet d'engager la responsabilité d'un hébergeur qui n'a pas retiré une information dénoncée comme illicite par un tiers **si celle-ci ne présente pas manifestement un tel caractère ou si son retrait n'a pas été ordonné par un juge [...]**⁵⁵⁸.*

L'idée est claire, et il est étonnant qu'elle ait été perdue de vue en France comme en Allemagne : seuls des propos dont l'illégalité crève les yeux peuvent faire l'objet d'une forme de censure privée. Lorsque naît l'hésitation, lorsqu'il existe une possibilité même infime que le propos visé soit par exemple une forme d'humour — même de mauvais goût — ou de contribution au débat public — même pauvre dans la forme et fruste sur le fond — il ne peut être question d'en exiger ni même

trisation=search.detail&year=2017&num=127&dLang=DE.

557. - V.supra, n°107.

558. - Décision n° 2004-496 DC du 10 juin 2004, considérant n° 9.

d'en admettre le retrait par quelques salariés d'une compagnie américaine. C'est au juge, doté de moyens suffisants par l'État, qu'il appartient de procéder à ces arbitrages vitaux dans une société démocratique.

Si l'insuffisante réactivité des plateformes face aux contenus haineux est un problème, un excès de zèle serait tout aussi inquiétant. L'enquête allemande, qui présente YouTube comme un bon élève, n'a pas cherché à savoir si cet opérateur supprimait avec la même vigueur des contenus dont la licéité portait à discussion, voire dont l'extrême mauvais goût était clairement compatible avec la liberté d'expression. Il serait pourtant intéressant de le savoir. Un renforcement très net des sanctions pesant sur sociétés exploitant ces outils de communication, voire sur les responsables des réseaux sociaux pris à titre personnel, présenterait en tous les cas un risque majeur de les pousser à pratiquer une censure excessive. Le responsable de la politique de modération du groupe aura rapidement arbitré entre le risque de se voir infliger une amende personnelle en millions d'euros, et celui de mécontenter un utilisateur en retirant un message pourtant licite. Aucune infraction pénale ne semble être commise par une plateforme trop diligente dans ses suppressions. Le seul risque est d'engager sa responsabilité civile à l'égard de l'utilisateur censuré. Constituera-t-il avocat pour obtenir en justice, des mois plus tard, que son message réapparaisse en ligne, à une date à laquelle il ne figurera plus dans les fils d'actualité de lecteurs⁵⁵⁹ ? La réponse est évidemment négative, et le seul frein à une politique trop conciliante d'un réseau social vis-à-vis des demandes de retrait est donc constitué par l'éventuelle mauvaise réputation que cela lui attirerait auprès de ses utilisateurs les plus attachés à la liberté d'expression.

Ces dangers ont été portés à l'attention du ministre allemand de la Justice, qui a décidé d'amender son projet. Il envisage notamment que les plateformes ne soient sanctionnées que s'il est démontré qu'elles ont été négligentes à plusieurs reprises⁵⁶⁰.

164. Une nouvelle infraction pénale ? - S'il a pu pêcher par excès de sévérité dans sa version initiale, le projet allemand n'est pas dépourvu d'intérêt pour le juriste français. Imaginons en effet qu'un intermédiaire technique manque à plusieurs reprises à ses obligations de retirer des contenus manifestement contraires à la loi, malgré des signalements. Sa responsabilité pénale peut-elle réellement être recherchée ? Sur quel fondement ? La loi sur la confiance dans l'économie numérique institue une immunité de responsabilité civile et pénale, assortie d'exceptions. On ne

559. - Nous avons déjà souligné, à propos du droit au déréférencement, que la question des recours est généralement considérée dans l'hypothèse où le moteur de recherche rechigne à retirer des informations. Mais la doctrine se préoccupe moins d'une politique de retrait zélée. V. supra, n° 107

560. - A. Shalal, « Germany waters down plan for social media fines over hate speech : Der Spiegel », dépêche Reuters du 4 avril 2017.

peut poursuivre l'intermédiaire, sauf s'il connaissait dès l'origine l'illicéité du contenu publié ou que cette illicéité a été portée à sa connaissance et qu'elle a tardé à réagir promptement. Cette exception au principe d'immunité pourrait sans difficulté être reformulée en une obligation positive, celle de réagir rapidement et de retirer les contenus signalés. Pour que l'on soit en présence d'une nouvelle infraction pénale, autonome, il faudrait non seulement que la loi soit ainsi formulée, mais encore qu'une peine ait été prévue en cas de manquement, ce qui n'est pas le cas⁵⁶¹. Dès lors, la doctrine pénaliste estime qu'il s'agit d'un « nouveau mode de participation par abstention à l'infraction d'autrui »⁵⁶². En ne supprimant pas un contenu appelant à la haine raciale, par exemple, Facebook se rendrait coupable de la même infraction que l'auteur du propos. Se pose alors un problème de temporalité, puisque les délits de presse sont commis instantanément lors de la publication, alors que le défaut de réaction de la plateforme est par hypothèse postérieur de plusieurs heures, jours, semaines ! On ne voit pas comment on pourrait être coauteur ou complice d'une infraction déjà entièrement consommée⁵⁶³.

L'approche allemande, qui consiste à ériger le défaut de réponse aux signalements en une infraction autonome, résout cette difficulté. Une fois le principe de cette infraction admis, il faut en affiner les éléments constitutifs et fixer la peine encourue.

Du point de vue des éléments constitutifs, il faut décider quels types de signalements sont pris en compte, et combien de temps ils doivent être restés sans réponse. S'agissant du « type de signalement », l'étude allemande démontre que les plateformes ne réagissent pas de la même manière selon qu'elles sont saisies au moyen d'un bouton *ad hoc* de signalement par un utilisateur ordinaire, par un utilisateur identifié, ou que les faits sont portés à sa connaissance moyennant un courrier - électronique ou papier. Le comportement de Twitter, qui supprime moins de 1% des contenus signalés par un utilisateur ordinaire, n'est pas si choquant une fois rappelés quelques éléments de contexte. Signaler un contenu par l'intermédiaire du bouton dédié est, sur ce réseau social, l'affaire de quelques instants. Il est fréquent de lire des propos d'utilisateurs qui se vantent d'avoir dénoncé un message uniquement parce qu'il contenait une option politique opposée aux leurs, ou parce qu'il provoquait leur agacement pour un motif quelconque. Pourtant, la loi fait du signalement d'un propos que l'on sait licite une infraction pénale, mais on ne trouve pas trace

561. - « Il est vrai qu'étant dépourvu de sanction pénale ce dernier texte n'établit pas une infraction spécifique nouvelle » : J. Francillon, « Messages racistes ou antisémites postés sur le réseau social Twitter », *RSC*, 2013, 566.

562. - *Ibid.*

563. - En ce sens, outre J. Francillon, art. préc. : E. Dreyer, « Les nouvelles responsabilités sur internet », *AJ pénal*, 2013, p. 15. Adde J. Bossan, « Le droit pénal confronté à la diversité des intermédiaires de l'Internet », art. préc., : « Il sera sans doute difficile de réunir les conditions de la responsabilité pénale et notamment de prouver l'intention infractionnelle ou la volonté de contribuer à l'infraction si la complicité est recherchée ».

jusqu'ici de poursuites sur ce fondement⁵⁶⁴. Dès lors, faire examiner l'ensemble des messages ayant recueilli un unique signalement par une équipe d'opérateurs humains requiert une débauche de moyens - sauf à adopter une politique de censure très large, dont la nocivité pour une société démocratique a déjà été dénoncée. Il peut sembler raisonnable alors de fixer un nombre minimal de signalements — avec tout l'arbitraire propre aux effets de seuils : deux, trois, cinq ? - avant que la plateforme n'ait l'obligation d'examiner le contenu. Toutefois, les utilisateurs « ordinaires » pourraient provoquer seuls l'examen du contenu en usant d'un moyen décourageant davantage les signalements fantaisistes, par exemple en remplissant un formulaire en ligne rappelant les sanctions encourues en cas de mensonge, auquel il faudrait attacher une copie d'une pièce d'identité. Quant aux utilisateurs de comptes identifiés, ils auraient chacun la capacité de provoquer, à eux seuls, l'examen du cas⁵⁶⁵. Il reste à fixer le délai dont disposera la plateforme pour réagir avant d'être en faute, plutôt que de faire appel à la notion de « prompt réaction », dont le flou est difficilement compatible avec le principe de légalité des délits et des peines. Rappelons ici que le projet allemand fixait ce délai à 24 heures.

Reste alors à définir une juste sanction. Tenir la plateforme pour coauteur des délits commis par les auteurs de contenus est non seulement techniquement difficile, comme cela a été démontré, mais de surcroît totalement inopportun. Les peines encourues pour un unique manquement seraient trop lourdes, et seraient prononcées à l'issue de procédures trop longues. Des amendes infligées aux intermédiaires par une autorité administrative semblent plus adaptées. La sanction pourrait être rapide - avec, bien sûr, des possibilités de recours devant le juge administratif. On peut imaginer un système dans lequel cette autorité reçoit copie électronique de tous les signalements ayant franchi les barrières imaginées précédemment (signalements collectifs d'utilisateurs ordinaires et signalements de « super-utilisateurs ») et restés sans réponse au bout de 24 heures. Sur simple constat de ce que certains contenus non filtrés étaient manifestement illicites, elle pourrait infliger une amende relativement légère par infraction constatée, tandis qu'une sanction plus lourde serait

564. - Art. 6, I, 4 de la loi précitée n° 2004-575 : « Le fait, pour toute personne, de présenter aux personnes mentionnées au 2 un contenu ou une activité comme étant illicite dans le but d'en obtenir le retrait ou d'en faire cesser la diffusion, alors qu'elle sait cette information inexacte, est puni d'une peine d'un an d'emprisonnement et de 15 000 Euros d'amende ». Il est frappant de constater que le législateur a fait de ce comportement une infraction, alors qu'il n'a pas songé à faire de même lorsque les plateformes restent inertes après un signalement d'authentique propos manifestement illicite. Quoi qu'il en soit, les poursuites seront rares : il faudrait que la plateforme fasse connaître le signalement factice aux autorités, et qu'on parvienne à démontrer la connaissance qu'avait l'internaute de ce que le propos n'était pas véritablement illicite, ce qui exige des efforts disproportionnés par rapport à la légèreté du trouble social créé. Enfin, la peine semble inadaptée, et devrait être remplacée par une amende.

565. - Une alternative consisterait à confier ce pouvoir d'alerte immédiate non pas à tous les utilisateurs identifiés, mais à une sélection d'associations reconnues d'utilité publique et dont l'objet statutaire est en lien avec la lutte contre les contenus haineux.

encourue après un certain nombre de manquements en une année. On songe ici non seulement à une amende d'un montant tout à fait dissuasif — calculée, par exemple, en proportion du chiffre d'affaires de l'entreprise -, mais aussi à une publication de sa condamnation auprès de l'ensemble de ses utilisateurs. L'autorité administrative chargée d'une telle mission reste à définir, car ni la CNIL, gardienne des données personnelles, ni le CSA, en charge de l'audiovisuel, n'ont vocation à l'assumer en l'état du droit. L'ensemble du système ainsi décrit permettrait que des sanctions effectives frappent les plateformes anormalement peu diligentes dans la lutte contre les contenus troublant gravement l'ordre social, sans pour autant noyer les juridictions.

C'est une chose de demander aux intermédiaires de la communication en ligne de retirer, de manière chirurgicale, les contenus illicites qui leur sont signalés sans toucher à la masse écrasante des publications conformes à la loi. C'en est une autre d'ordonner le blocage d'un site dans son entier.

B - Le blocage d'un site Internet par les fournisseurs d'accès

165. **Une mesure exceptionnelle** - Lorsqu'un propos franchissant nettement les limites de la liberté d'expression est présent sur les pages d'un réseau social ou d'un moteur de recherche, au milieu d'informations parfaitement licites et ayant d'autres auteurs, la juste solution consiste à en exiger le retrait par la plateforme, à défaut d'avoir obtenu de l'auteur lui-même qu'il y procède. Mais laissons les plateformes de côté et considérons à présent un site Internet classique : un individu ou un groupe d'individus a la maîtrise de son contenu, qu'on supposera gravement illicite. Il peut arriver que les auteurs et éditeurs échappent à l'imperium de la justice française, par exemple parce qu'ils ont réussi à s'assurer un anonymat qui résiste aux investigations, ou qu'ils se situent dans un pays dont le système judiciaire ne coopère pas avec le nôtre. Il faut encore imaginer que l'hébergeur lui-même est hors d'atteinte, car à défaut il suffirait de lui signaler l'illicéité manifeste pour qu'il soit tenu de réagir, en vertu des principes précédemment décrits. Il sera toujours possible d'obtenir le déréférencement dans les grands moteurs de recherche qui, eux, ne peuvent se soustraire à notre système juridique - du moins s'agissant des consultations effectuées depuis notre territoire⁵⁶⁶. Mais cela ne fera qu'accroître la difficulté à trouver les contenus, sans empêcher leur consultation par ceux qui disposent au préalable de leur adresse. Dans un tel cas de figure, le dernier recours consiste à exercer une contrainte sur les FAI : eux sont soumis à la juridiction française, et constituent un point de passage obligatoire entre leurs abonnés et le réseau. D'un point de vue

566. - Sur la lutte entre la CNIL et Google visant à soumettre même les résultats proposés aux internautes hors de l'Union à la jurisprudence de la CJUE, V.supra, n°108. S'agissant des sites terroristes et pédopornographiques, le déréférencement peut être ordonné par l'administration, en vertu du décret n° 2015-253.

technique, il s'agit d'obliger les FAI à intervenir sur leurs serveurs Domain Name System (le DNS)⁵⁶⁷. Lorsqu'un internaute tape une adresse sous forme de lettres dans son navigateur (par exemple www.u-picardie.fr), le serveur DNS consulte sa base de données pour savoir à quelle adresse IP chiffrée cela correspond (par exemple 193.49.184.17). Il fournit ensuite cette information au navigateur, qui peut alors établir la connexion. Le DNS est donc une sorte d'annuaire, dont il est possible de fausser le contenu pour qu'il guide l'internaute à la recherche d'un site djihadiste, par exemple, vers une page l'avertissant de ce que ce site a été interdit d'accès. La mesure peut être contournée, mais elle rend l'accès à ces contenus pénible et difficile⁵⁶⁸.

166. **Les blocages judiciaires** - On se souvient qu'au nombre des dispositions communes aux FAI et aux hébergeurs, il fallait compter celle-ci : « L'autorité judiciaire peut prescrire en référé ou sur requête [...] toutes mesures propres à prévenir un dommage ou à faire cesser un dommage occasionné par le contenu d'un service de communication au public en ligne »⁵⁶⁹. Le Code de procédure civile ne fournissait-il pas à lui seul toutes les ressources nécessaires, par exemple en posant que : Le président peut toujours, même en présence d'une contestation sérieuse, prescrire en référé les mesures conservatoires ou de remise en état qui s'imposent, soit pour prévenir un dommage imminent, soit pour faire cesser un trouble manifestement illicite »⁵⁷⁰ ? Mais le texte de la loi pour la confiance dans l'économie numérique apporte cette précision fondamentale : le juge ne pourra s'adresser au FAI qu'à défaut de possibilité de contraindre l'hébergeur⁵⁷¹. La disposition spéciale l'emporte sur la disposition générale et cette subsidiarité devra donc être respectée⁵⁷². Des

567. - W. Audureau et S. Seelow, « Comment fonctionnent les blocages de sites djihadistes », article *lemonde.fr* du 17 mars 2015.

568. - Sur l'ensemble de la question des blocages de site internet, V. not. M. Quémener, « Sites internet. Retrait, blocage, déréférencement », fasc. 690 in *JurisClasseur communication*, 24 mai 2016 ; E. Dreyer, « Le blocage de l'accès aux sites terroristes ou pédopornographiques », *JCP G*, 6 avr. 2015, doct., 423.

569. - Art. 6, I, 8 de la loi n° 2004-575 précitée. Sur les règles communes aux FAI et aux hébergeurs, V. supra, n° 158 et s.

570. - Art. 809 al. 1.

571. - « L'autorité judiciaire peut prescrire en référé ou sur requête, **à toute personne mentionnée au 2 ou, à défaut, à toute personne mentionnée au 1**, toutes mesures propres à prévenir un dommage ou à faire cesser un dommage occasionné par le contenu d'un service de communication au public en ligne » (souligné par nous).

572. - V. par ex. l'ordonnance de référé du président du TGI de Paris du 15 septembre 2014, n° 14/55416 : les dispositions de l'ordonnance de référé visant les FAI « devront être mises en œuvre à défaut d'exécution [par l'hébergeur] des mesures mises à sa charge, sur simple disposition du président de l'AMF exposant les conditions dans lesquelles [l'hébergeur] s'est absten[u] ou a cessé de se conformer aux injonctions qui lui sont faites par ailleurs dans le délai fixé au dispositif » (ordonnance consultable sur <https://cdn2.nextinpact.com/medias/20140915-amf-ordonnance-refere-tgi-paris.pdf>).

textes plus spéciaux encore prévoient l'arrêt judiciaire d'un service de communication en ligne : la loi de 1881⁵⁷³ ou encore la loi sur les jeux d'argent en ligne⁵⁷⁴.

167. Les blocages administratifs - Alors même que les procédures en référé ou sur requête se caractérisent, en principe, par leur célérité et leur efficacité, le choix a été fait par les pouvoirs publics d'autoriser les blocages de sites par la seule autorité administrative, en certains contextes. En matière de lutte contre la provocation à des actes terroristes, contre l'apologie de tels actes et contre la diffusion de contenus à caractère pédopornographique, la loi prévoit ainsi une procédure particulière⁵⁷⁵. L'autorité administrative doit adresser sa demande de retrait aux éditeurs ou hébergeurs du site concerné. Elle informe simultanément les FAI de cette démarche, qui se tiennent prêts pour l'éventuelle étape suivante. En l'absence de retrait des contenus litigieux dans un délai de 24 heures, en effet, le blocage administratif sera imposé aux fournisseurs d'accès, qui doivent alors obéir « sans délai ». Si le site Internet ne précise pas, ainsi que la loi l'exige pourtant, l'identité des responsables de la publication, l'autorité contactera les FAI sans attendre. Les moteurs de recherche et annuaires peuvent être sommés de cesser le référencement des adresses électroniques concernées⁵⁷⁶. Enfin, une personne qui dupliquerait les contenus du site bloqué afin de les rendre à nouveau accessibles, en connaissance de cause, commettrait une infraction pénale spécifique, durement réprimée⁵⁷⁷.

L'abus de telles procédures ne serait pas sans danger, dans une société démocratique. Pour se prémunir contre ces critiques, le législateur a prévu que la CNIL devrait désigner, en son sein, une personnalité qualifiée pour qu'elle soit destinataire d'une copie des demandes de retrait⁵⁷⁸. Cette personnalité peut recommander à l'autorité administrative de mettre fin à une procédure qui lui

573. - Art. 50-1 de la loi de 1881 précitée : « Lorsque les faits visés par les articles 24 et 24 bis, par les deuxième et troisième alinéas de l'article 32 et par les troisième et quatrième alinéas de l'article 33 résultent de messages ou informations mis à disposition du public par un service de communication au public en ligne et qu'ils constituent un trouble manifestement illicite, l'arrêt de ce service peut être prononcé par le juge des référés, à la demande du ministère public et de toute personne physique ou morale ayant intérêt à agir ».

574. - Art. 61 de la loi n° 2010-476 du 12 mai 2010 relative à l'ouverture à la concurrence et à la régulation du secteur des jeux d'argent et de hasard en ligne, qui prévoit une procédure et des délais spécifiques à la matière.

575. - Art. 6-1 de la loi n° 2004-575 précitée, issu de la loi n° 2014-1353 du 13 novembre 2014 renforçant les dispositions relatives à la lutte contre le terrorisme.

576. - Sans cela, les internautes suffisamment compétents et motivés, découvrant sur les annuaires ou moteurs de recherche l'existence de contenus bloqués, pourraient y accéder tout de même. Il est en effet possible d'utiliser des serveurs DNS situés hors de l'emprise des pouvoirs publics français, ou le navigateur du réseau TOR.

577. - Art. 421-2-5-1 du Code pénal : « Le fait d'extraire, de reproduire et de transmettre intentionnellement des données faisant l'apologie publique d'actes de terrorisme ou provoquant directement à ces actes afin d'entraver, en connaissance de cause, l'efficacité des procédures prévues à l'article 6-1 de la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique ou à l'article 706-23 du code de procédure pénale est puni de cinq ans d'emprisonnement et de 75 000 € d'amende ».

578. - Art. 6-1 al. 2 de la loi n° 2004-575 précitée.

semblerait irrégulière et, à défaut d'être entendue, saisir le juge administratif. Elle rédige chaque année un rapport « sur les conditions d'exercice et les résultats de son activité, qui précise notamment le nombre de demandes de retrait, le nombre de contenus qui ont été retirés, les motifs de retrait et le nombre de recommandations faites à l'autorité administrative »⁵⁷⁹. Celui-ci est rendu public, mais aussi remis au Gouvernement et au Parlement⁵⁸⁰.

168. Blocages de sites et libertés fondamentales - Le dispositif français, en particulier la possibilité offerte à l'administration d'obtenir directement que des sites soient rendus inaccessibles, porte-t-il une atteinte excessive aux libertés publiques ? Le Conseil constitutionnel ne semble pas le penser. Le consensus parlementaire relatif à la législation antiterroriste a conduit à ne pas déférer la loi de novembre 2014 aux Sages dans le cadre de leur contrôle a priori - une QPC pourrait être posée à l'avenir. En revanche, le blocage administratif des sites à caractère pédopornographique avait été soumis à son examen⁵⁸¹.

Considérant, en second lieu, que les dispositions contestées ne confèrent à l'autorité administrative que le pouvoir de restreindre, pour la protection des utilisateurs d'Internet, l'accès à des services de communication au public en ligne lorsque et dans la mesure où ils diffusent des images de pornographie infantile ; que la décision de l'autorité administrative est susceptible d'être contestée à tout moment et par toute personne intéressée devant la juridiction compétente, le cas échéant en référé ; que, dans ces conditions, ces dispositions assurent une conciliation qui n'est pas disproportionnée entre l'objectif de valeur constitutionnelle de sauvegarde de l'ordre public et la liberté de communication garantie par l'article 11 de la Déclaration des droits de l'homme et du citoyen de 1789⁵⁸² [...].

Quant à la jurisprudence de la Cour européenne des Droits de l'Homme, elle a pu sanctionner des blocages trop grossiers survenus en Turquie, qui touchaient des plateformes entières - par exemple, l'ensemble de YouTube, un hébergeur de vidéos, ou l'ensemble de Google Sites, un hébergeur de milliers de sites Internet⁵⁸³. La France échappe sans doute à de telles critiques.

579. - Al. 4 du même texte.

580. - Le rapport de 2015 rédigé par M. Alexandre Linden fait par exemple état, à la date du 29 février 2016, de 312 demandes de blocage de sites, 1439 demandes de retrait de contenus et 855 demandes de déréférencement d'adresses de sites. Il est précisé que le terrorisme représente 2/3 de l'activité, à la suite des attentats de novembre 2015. Le rapport est consultable à l'adresse : https://www.cnil.fr/sites/default/files/atoms/files/cnil_rapport_blocage_sites_internet_2016_0.pdf.

581. - Article 4 de la loi n° 2011-267 du 14 mars 2011 d'orientation et de programmation pour la performance de la sécurité intérieure.

582. - Considérant 8 de la décision n° 2011-625 DC du 10 mars 2011.

583. - CEDH, 18 déc. 2012, *Ahmet Yildirim c. Turquie*, n° 3111/10 ; CEDH, 1er déc. 2015, *Cengiz et autres c. Turquie*, n° 48226/10. Outre le caractère excessivement large des blocages, ceux-ci n'avaient pas de base légale en droit turc, autre circonstance qui éloigne les décisions judiciaires condamnées du système ayant cours en France.

Mais ce n'est pas parce que le dispositif français échappe aux griefs d'inconstitutionnalité et d'inconventionnalité qu'il échappe à la critique. Dans un avis, le Conseil national du numérique a fait part de ses vives réserves. Il conteste l'utilité même des blocages : « dans un contexte de lutte contre les stratégies de diffusion d'idéologies radicales, le recours au blocage peut avoir un effet contreproductif en attisant l'envie de consulter les contenus bloqués »⁵⁸⁴. Il est difficile au juriste de se prononcer sur le bien-fondé d'une accusation qui dépasse de loin son champ disciplinaire. En revanche, une autre critique du CNNum, spécifiquement dirigée contre les blocages administratifs mérite l'attention :

*Les consultations conduites par le Conseil ont mis en évidence que le nombre de sites de recrutement se limite à une fourchette comprise entre une dizaine et une centaine, selon les experts. Au regard de ces chiffres, le risque de surcharge des tribunaux parfois évoqué n'est pas caractérisé et il n'apparaît pas raisonnable de créer un dispositif spécifique contournant l'autorité judiciaire au profit de l'autorité administrative*⁵⁸⁵.

Cette remarque est parfaitement convaincante. En ces temps d'état d'urgence, le juge judiciaire semble peu à peu dépossédé de son rôle traditionnel de gardien des libertés publiques. L'administration, qui traîne dans son sillage sa propre justice, serait seule apte à mener des combats efficaces contre les plus violents agresseurs de notre société. Ce postulat inquiète, et il n'est pas démontré.

Les obligations des intermédiaires techniques en matière de suppression des contenus illicites ayant été envisagées, il est temps d'examiner le rôle fondamental qu'ils jouent dans la mise en forme de l'information.

II - L'agencement de l'information

169. **Du choix éditorial au filtre algorithmique** - Les intermédiaires de la communication en ligne ont un rapport très passif à l'information qu'ils véhiculent, si on les compare au rôle qu'endosse traditionnellement un directeur de publication ou un éditeur. L'impact de cette évolution sur le traitement des contenus manifestement illicites a été souligné. Là où l'intervention *a priori* de personnes humaines identifiées et personnellement responsables constituait une barrière dense, les intermédiaires numériques se contentent de réagir ponctuellement et après coup, lorsque les utilisateurs leur tirent la manche ou que les autorités leur en donnent l'ordre. Des milliers de contenus ostensiblement illégaux passent au travers des mailles de cet étrange filet.

584. - Conseil National du numérique, *Avis n° 2014-3 du 15 juillet 2014 sur l'article 9 du projet de loi renforçant les dispositions relatives à la lutte contre le terrorisme*.

585. - *Ibid.*

Cette différence d'approche se prolonge lorsque l'intermédiaire numérique fait profession non seulement de véhiculer l'information, mais aussi de la mettre en forme et de la placer directement au contact de ses destinataires. Ce n'est pas le rôle d'un fournisseur d'accès, par exemple, ni celui d'un pur hébergeur, mais c'est bien celui d'un réseau social ou d'un moteur de recherche. Le rôle de l'éditeur classique consiste, à partir d'un espace de publication limité, à procéder à des choix. Prendre personnellement connaissance des contenus candidats à la publication lui permet non seulement d'écarter ceux qui dépassent nettement les limites de la liberté d'expression, et qui risqueraient de lui valoir une condamnation pénale, mais surtout de retenir une sélection, un ordre, une hiérarchie de l'information, produisant ainsi un discours conscient et assumé sur le monde.

Le réseau social ou le moteur de recherche dispose, quant à lui, d'un espace potentiellement infini pour afficher des publications ou des résultats. Aucun employé humain n'est chargé d'intervenir directement ni sur le périmètre ni sur l'ordre de ce qui s'affiche sur l'écran d'un utilisateur donné. Pour autant, ce n'est pas une matière brute qui est livrée à l'internaute. L'information n'est pas travaillée par l'homme, mais elle est filtrée, classée et positionnée par les machines. Cela est particulièrement évident s'agissant d'un moteur de recherche généraliste, où ces opérations ne sont pas le résultat d'un choix, mais une nécessité. Il n'existe pas d'ordre objectif ou naturel dans lequel les réponses à une requête donnée devraient s'afficher. Quelle est la page susceptible d'intéresser le plus un internaute interrogeant Google ou Qwant sur « Marcel Proust », « plus belle plage du monde » ou « conseils pour réussir ses études de droit » ? Il n'existe aucune réponse définitive et parfaite. En amont, un algorithme aura été conçu par ces sociétés, un ensemble d'opérations visant à manipuler des informations, une machine à pétrir la connaissance. C'est une boîte noire : un problème à résoudre y entre, une réponse en sort, et la qualité de cette réponse est soumise au jugement personnel de chaque utilisateur. De leur satisfaction dépend leur fidélité ; de leur fidélité dépendent les revenus publicitaires sur lesquels repose une large part du modèle économique de ces compagnies. Mais les moteurs de recherche ne sont pas les seuls concernés. Les réseaux sociaux n'ont théoriquement pas l'obligation d'y recourir. En effet, il existe pour eux une manière objective d'afficher l'information, par exemple en montrant à chaque utilisateur l'intégralité des contenus publiés par ses contacts, dans un ordre purement chronologique. Il y a un risque : plus ces réseaux gagnent en popularité, plus un individu donné aura « d'amis », et plus son fil d'actualités grossira, jusqu'à ce qu'il se noie dans un flux ininterrompu de publications, d'interactions et de commentaires. Dans cette masse d'informations, le risque est grand qu'une partie ne l'intéresse, ne l'amuse ni ne le stimule d'aucune façon. Il se connectera alors au réseau de plus en plus rarement, et finira par l'abandonner sans même s'en apercevoir. Le problème ne se

pose plus s'il est possible de prédire quels contenus il aura plaisir à consulter, pour les lui proposer exclusivement ou en priorité. C'est le choix opéré de longue date par le réseau dominant, Facebook.

Les actualités qui s'affichent dans votre fil d'actualité sont sélectionnées en fonction de votre activité et de vos contacts sur Facebook. Vous pouvez voir ainsi davantage d'actualités susceptibles de vous intéresser, notamment celles des amis avec lesquels vous communiquez le plus. L'affichage d'une actualité dans votre fil d'actualité dépend notamment du nombre de commentaires et de mentions « J'aime » qu'elle reçoit, ainsi que de sa nature (par exemple, s'il s'agit d'une photo, d'une vidéo ou d'un nouveau statut)⁵⁸⁶.

Le réseau Twitter, après avoir longtemps retenu un système d'affichage exhaustif et purement chronologique des contenus, s'est finalement doté à son tour d'un algorithme de discrimination⁵⁸⁷.

170. Un pouvoir sans responsabilité ? - Ainsi, consulter un résultat de recherche ou un réseau social, ce n'est plus dialoguer avec l'intellect d'un directeur de publication, mais se présenter devant une machine, un distributeur automatique d'information « pertinente ». Cette évolution n'est pas sans conséquence juridique, comme le montre une affaire restée fameuse sous le nom de « Google Suggest ». Cette fonctionnalité du moteur de recherche orientait non pas les résultats de recherche, mais les questions qui lui étaient posées. Au fur et à mesure que la requête était saisie, le moteur formulait un certain nombre de propositions jugées statistiquement probables sur ce que serait la suite de la question. Du point de vue qui nous intéresse, le mécanisme est comparable à celui qui classe les résultats de la recherche. Dans les deux cas, il s'agit d'apporter à l'internaute une information jugée pertinente pour lui, en se fondant sur l'intérêt manifesté par tous ceux qui l'ont précédé dans la même voie. Le panurgisme de l'algorithme fait sa force, en indiquant à celui qui le consulte où se dirige la majorité, mais il est aussi sa faiblesse : lorsque les masses prennent une direction qui devrait l'alerter, il les suit sans guère hésiter. En l'espèce, un grand nombre d'internautes avait soumis des requêtes associant le nom d'une société et le terme « escroc ». *Suggest* en avait pris acte, et proposait à toute personne saisissant le nom de l'entreprise d'y accoler ce terme indubitablement injurieux. Le moteur de recherche avait été condamné par une cour d'appel, de même que son directeur de la publication, aussi sévèrement que si ce dernier avait dirigé un journal.

[...] le fait de diffuser auprès de l'internaute l'expression « lyonnaise de garantie, escroc » correspond à l'énonciation d'une pensée rendue possible uniquement par la mise en œuvre de la fonctionnalité en cause, qu'il est acquis aux débats que les suggestions proposées aux internautes procèdent des sociétés Google à partir d'une

586. - Extrait de la page « comment fonctionne le fil d'actualité ? » : <http://www.facebook.com/help/327131014036297/>.

587. - V. par ex. W. Oremus (trad. A. Bourguilleau), « Voici comment fonctionne l'algorithme de Twitter », article *Slate.fr* du 10 mars 2017.

*base de données qu'elles ont précisément constituée pour ce faire, lui appliquant des algorithmes de leur fabrication, que le **recours à ce procédé n'est que le moyen d'organiser et de présenter les pensées que la société Google met en circulation sur le réseau interne***⁵⁸⁸.

Cette décision a été censurée par la Cour de cassation.

*[...] en statuant ainsi, quand la fonctionnalité aboutissant au rapprochement critiqué est **le fruit d'un processus purement automatique** dans son fonctionnement et aléatoire dans ses résultats, de sorte que l'affichage des « mots-clés » qui en résulte est **exclusif de toute volonté** de l'exploitant du moteur de recherche d'émettre les propos en cause ou de leur conférer une signification autonome au-delà de leur simple juxtaposition et de leur seule fonction d'aide à la recherche, la cour d'appel a violé [les articles 29 et 33 de la loi de 1881]*⁵⁸⁹.

La cour d'appel soulignait le rôle essentiel du moteur de recherche dans la circulation et la mise en scène de l'information. Elle se situait sur le terrain du pouvoir procuré par l'algorithme et sur les conséquences de son fonctionnement. La Cour de cassation, à l'inverse, met en avant ses ressorts internes. En effet, les délits de presse considérés ne peuvent être commis que si un élément intentionnel est retenu. Certes, s'il n'a pas de volonté propre, un algorithme peut être le véhicule d'une intention de la part de ses concepteurs - techniquement, rien n'empêche de favoriser sciemment des requêtes de recherche injurieuses ou racistes, par exemple. Mais tel n'était pas le cas en l'espèce, puisqu'il était le miroir fidèle des questions antérieurement formulées par la majorité. Si la solution retenue par la Cour se comprend, en ce qu'elle est cohérente avec les exigences de la matière pénale, elle fait naître de difficiles questions. D'abord, comment s'assurer concrètement de la neutralité de l'algorithme par rapport au fond des messages qu'il manipule, puisque leur code est généralement inconnu ? Ensuite, quand bien même cet ensemble d'opérations informatiques serait intrinsèquement neutre, l'affaire *Google Suggest* rappelle que son fonctionnement produit parfois des effets néfastes pour l'harmonie sociale. L'effet puissant de ces ensembles d'opérations mathématiques sur la manière dont les citoyens s'informent et communiquent incite à surmonter — sans l'ignorer — l'argument de l'automaticité pour mieux ouvrir certains débats.

Récemment, des critiques ont surgi dans deux directions précises : l'excès de personnalisation de l'information par les algorithmes (A) et leur insuffisante sensibilité à la véracité de l'information présentée (B).

588. - CA Paris, 14 décembre 2011, N° 11/15029, dans la version ramassée qu'en donne Cass. 1ère civ., 19 juin 2013, n° 12-17.591. Souligné par nous.

589. - Cass. 1ère civ., 19 juin 2013, n° 12-17.591 : JCP G, 2013, 907, note A. Lepage. Souligné par nous.

A - La personnalisation des contenus

171. **Le biais de confirmation** - Un premier reproche actuellement adressé aux algorithmes de sélection et de présentation d'informations consiste à dire qu'ils opèrent une personnalisation excessive des contenus. Dans le fonctionnement décrit ci-dessus de *Google Suggest*, il a été supposé que les propositions formulées seraient les mêmes pour tous les internautes tapant le début d'une question adressée au moteur. En réalité, la plupart du temps, les algorithmes se fondent sur ce qu'ils savent de la personne précise qui les interroge pour lui répondre. Ils se servent pour cela des données personnelles accumulées sur son compte par le passé⁵⁹⁰. Un haut responsable de Google France en proposait un exemple⁵⁹¹. S'il se contente de saisir dans le moteur de recherche de son entreprise une suite de caractères en apparence absconse, comme « C-362/14 », l'algorithme comprendra qu'il s'agit d'un numéro d'arrêt rendu par la Cour de justice de l'Union européenne, car cet utilisateur déterminé a l'habitude de consulter le site de la juridiction. La même requête formulée par une personne ayant d'autres centres d'intérêt conduira à des résultats différents. L'exemple est innocent, et met en scène la capacité — réelle — de ces techniques à faire économiser à leurs utilisateurs du temps et de l'énergie, en devançant leurs désirs et en se contentant d'indications fragmentaires pour fournir un service performant. Mais une illustration politiquement moins neutre en révèle les dangers. Selon un auteur américain, Eli Pariser, si une personne politiquement marquée à droite et une autre plutôt à gauche lancent une recherche Google sur les lettres « BP », « La première reçoit, en tête de page, des informations sur les possibilités d'investir dans la British Petroleum, la seconde sur la dernière marée noire qu'a causée la compagnie pétrolière britannique »⁵⁹². Il qualifie ce phénomène, qui consiste à regarder la réalité de manière différenciée au travers des algorithmes, de « bulle de filtres »⁵⁹³. Il poursuit sa démonstration en l'étendant à Facebook, où les automatismes chargés de trier les publications de l'ensemble de ses amis pour en extraire ce qu'il aura le plus de plaisir à lire ont peu à peu fait disparaître ceux de ses contacts dont il ne partageait pas les conceptions⁵⁹⁴. Sa tendance à moins ouvrir les liens qu'ils proposaient et à moins leur accorder de « j'aime » aurait été repérée et amplifiée par le réseau

590. - V. *supra*, n° 50 et s.

591. - Exemple donné à la tribune par M. Francis Donnat, alors directeur des politiques publiques de Google France, lors d'une conférence du 7 décembre 2015 sur « Enjeux juridiques, économiques et sociaux du numérique » organisée par la Société de Législation Comparée.

592. - F. Joignot, « Sur internet, l'invisible propagande des algorithmes », article *lemonde.fr* du 15 septembre 2016. L'exemple est tiré de E. Pariser, *The filter bubble : how the new personalized web is changing what we read and how we think*, Penguin books, 2012.

593. - Du nom de l'ouvrage précité *The filter bubble*.

594. - *Ibid.*

social. Il y a deux manières de voir cet exemple : soit l'algorithme s'est contenté de rendre visible un comportement préexistant visant à éviter l'inconfort intellectuel, soit il l'a amplifié.

Cette stratégie d'esquive des idées contrariant notre vision du monde n'est effectivement pas nouvelle dans son principe. Elle est connue en psychologie sous le nom de « biais de détermination », et Francis Bacon la décrivait très bien il y a près de quatre siècles.

*The human understanding when it has once adopted an opinion (either as being the received opinion or as being agreeable to itself) draws all things else to support and agree with it. And though there be a greater number and weight of instances to be found on the other side, yet these it either neglects and despises, or else by some distinction sets aside and rejects, in order that by this great and pernicious predetermination the authority of its former conclusions may remain inviolate [...]*⁵⁹⁵.

172. **L'amplification du biais par les algorithmes** – Une fois encore, les technologies numériques se contentent donc d'exacerber une difficulté très ancienne. Comme le relève M. Dominique Cardon, à propos du fil d'actualités de Facebook : « [...] ce sont les utilisateurs qui, à travers les liens sur lesquels ils choisissent de cliquer, referment la bulle sur eux-mêmes. Les libéraux lisent des informations libérales et les conservateurs des informations conservatrices »⁵⁹⁶. Pour lui, cela n'empêche pas la critique de ces technologies, mais la déplace.

*C'est en effet le comportementalisme radical des nouvelles techniques de calcul qu'il faut questionner. Avec une insistance provocante, les concepteurs des algorithmes prédictifs ne cessent de dire qu'ils ne font que s'appuyer sur les comportements passés de l'internaute pour lui recommander des choses à faire [...] Le comportementalisme radical joue ce rôle à la fois lucide et démoralisant de démontrer à des sujets qui pensaient s'être émancipés des déterminations que, en ce qu'ils pensent être des singularités inassignables, ils continuent à être prévisibles, petites souris mécaniques dans les griffes des calculateurs*⁵⁹⁷.

Les arguments des promoteurs des algorithmes de personnalisation ont une portée essentiellement pratique : il s'agit de rendre la navigation rapide, efficace, performante. L'utilisateur ne fait qu'emprunter des raccourcis à travers le maquis informationnel, et arrive sans attendre à destination. Eût-il passé des heures à se promener à travers les contenus, c'est là qu'il se serait arrêté pour finir : la machine le sait mieux que lui, car elle le connaît mieux qu'il se connaît lui-même. Alors, pourquoi perdre son temps ? En réalité, ce discours est sous-tendu par une véritable vision politique de ce qu'est l'acte de s'informer, et plus fondamentalement encore de ce qu'est l'être humain.

L'algorithme, pourtant, n'est pas infallible, et M. Cardon en propose un exemple.

595. - F. Bacon, *The new organon*, 1620, XLVI.

596. - D. Cardon, *À quoi rêvent les algorithmes ? Nos vies à l'heure des big data*, Seuil, 2015.

597. - *Ibid.*

Latanya Sweeney, une chercheuse en informatique afro-américaine, a remarqué que, lorsqu'elle tapait son nom dans le moteur de recherche de Google, elle voyait apparaître la publicité « Latanya Sweeney arrested ? ». Cette publicité propose un service de consultation en ligne [...] qui permet [...] de savoir si les personnes ont un casier judiciaire. Or, le nom de ses collègues blancs n'était pas associé au même type de publicité [...]. (L'algorithme) ne comporte pas de règle lui demandant de détecter les personnes noires et les personnes blanches. Il se contente de laisser faire les régularités statistiques qui font que les noms et prénoms des personnes noires sont statistiquement plus souvent liés à des recherches de casier judiciaire. Livré à lui-même, le calculateur s'appuie sur les comportements des autres internautes et contribue, « innocemment », si l'on ose dire, à la reproduction de la structure sociale, des inégalités et des discriminations⁵⁹⁸.

Il serait facile de qualifier cet exemple de pathologique, d'y voir un simple raté, et de l'écarter en conséquence d'un revers de la main.

Ce serait passer à côté de ce qu'il révèle de très profond dans le fonctionnement des algorithmes de personnalisation. Il est au contraire très riche d'enseignements, car il donne à voir, en le grossissant, un défaut d'approche habituellement plus discret. Lorsqu'il détermine quel maître il doit saisir, l'automatisme n'a pas la capacité de saisir l'individu ni les groupes auxquels il appartient dans toute leur complexité. Deux approches sont alors possibles, l'une déductive, l'autre inductive. L'approche déductive consiste à établir un « profil » de l'utilisateur qui comprendra par exemple certains centres d'intérêts majeurs, un historique de ses habitudes de consommation, des orientations politiques. Il en résulte au mieux une épure, au pire une caricature, dans tous les cas une extrême simplification du réel. L'autre approche est inductive, et repose sur la notion déjà évoquée de big data. Si des milliers d'individus ont en commun d'avoir acheté trois livres A, B, C et qu'un algorithme de recommandation se trouve face à un utilisateur n'ayant acheté qu'A et B, il va recommander C. Cette règle aura été construite à partir d'une pure série d'observations, sans qu'on ne cherche jamais à y accoler une tentative d'explication. C'est un monde de « corrélations sans causalité » qui se prépare, dont Mme Sweeney a été victime et contre lequel M. Cardon met en garde⁵⁹⁹.

Notre société n'a pas attendu les algorithmes pour se fragmenter en sous-groupes qui communiquent trop peu. Mais les filtres numériques, qu'ils procèdent par portraits-robots ou par pures corrélations, risquent d'accentuer ces ruptures et de les rendre irréversibles. Des visions du monde qui se rencontraient peu ne se croiseront jamais. Chacun, dans sa vie en ligne, sera placé dans un cocon d'informations qui exacerberont sa vision du monde sans jamais heurter ses goûts. À un niveau individuel, l'individu sera perpétuellement ramené, par des mécanismes discrets et

598. - D. Cardon, *op. cit.*, p. 84.

599. - *Ibid.*

infatigables, à la position intellectuelle qui était la sienne par le passé. Les algorithmes dits « prédictifs » ne prévoient pas comment une personne peut évoluer, mais seulement comment elle s'apprête à réagir si elle reste strictement égale à elle-même sa vie durant.

Faut-il y voir une prise de conscience ? YouTube diffusait durant la campagne présidentielle française de 2017, une vidéo intitulée « Forgeons nos opinions. Découvrez d'autres opinions pour faire avancer le débat »⁶⁰⁰. L'initiative est louable, mais il faudrait aller un peu plus loin.

173. Révéler sans interdire – Personne n'a songé à forcer les lecteurs de Libération à souscrire un abonnement au Figaro, ou les admirateurs d'Adam Smith à ouvrir le Capital. S'il est toujours souhaitable que les citoyens s'exposent en permanence à différentes visions du monde, il n'est pas question de les y contraindre. Mais lorsqu'il s'abonne à un journal ou qu'il parcourt l'œuvre d'un auteur identifié, l'individu a certainement une conscience même confuse de ce qu'il a effectué un choix, au sein de l'univers des informations qui lui sont offertes. Chez le buraliste, ou sur les étals du libraire, les idées concurrentes s'étalent, à portée de main. Les ignorer, c'est prendre une décision. Une promenade dans un univers numérique « personnalisé » fait oublier jusqu'à l'existence d'alternatives, qui ne se présenteront même plus au regard. Les publications « adverses », dont il eût été profitable de voir passer tout de même le titre et un résumé, auront été éliminées à force de n'avoir jamais été ouvertes et manipulées longuement. À ce caractère souterrain de l'impact des algorithmes, s'ajoute la difficulté à vérifier s'ils ne sont pas tout simplement biaisés par leurs concepteurs, qui chercheraient non pas à enfermer l'individu pour toujours dans un concentré de lui-même, mais à influencer son jugement, petit à petit, dans le sens d'une opinion particulière. L'enjeu n'est donc pas d'interdire ces techniques de personnalisation, mais de rendre l'internaute conscient de ce que l'information qui lui est adressée est biaisée – au sens neutre de ce terme, car ce biais peut fort bien lui convenir. Afin de rendre le biais observable, deux directions complémentaires peuvent être explorées : en révéler les critères ; permettre qu'il soit contourné.

Une première direction consiste à mettre au jour les critères utilisés par les plateformes. Depuis la loi République numérique, ces acteurs ont l'obligation de procéder par eux-mêmes à la révélation des principaux facteurs influant sur leur sélection de l'information. Le Code de la consommation dispose en effet :

II. – Tout opérateur de plateforme en ligne est tenu de délivrer au consommateur une

600. - Vidéo du 9 avril 2017 (<https://youtu.be/gWsG-6vyqfo>). Il n'est toutefois pas certain qu'il s'agisse d'une campagne contre le repli intellectuel engendré par la bulle filtrante : le propos essentiel est d'encourager les utilisateurs à s'abonner aux « chaînes » de certains stars de la plateforme de vidéos en ligne, afin de s'exposer à la diversité d'opinions qu'ils sont supposés véhiculer.

information loyale, claire et transparente sur :

1° Les conditions générales d'utilisation du service d'intermédiation qu'il propose et sur les modalités de référencement, de classement et de déréférencement des contenus, des biens ou des services auxquels ce service permet d'accéder ;

2° L'existence d'une relation contractuelle, d'un lien capitalistique ou d'une rémunération à son profit, dès lors qu'ils influencent le classement ou le référencement des contenus, des biens ou des services proposés ou mis en ligne (...)»⁶⁰¹.

Un décret, qui n'a pas encore été pris, doit préciser les conditions d'application de ce texte « en tenant compte de la nature de l'activité des opérateurs de plateforme en ligne ». Mais comment vérifier que les informations fournies par les professionnels sont justes et exhaustives, que rien n'est dissimulé ? Le contenu précis de l'algorithme, lorsqu'il est exploité par un acteur privé, est un secret de fabrication : il n'est pas révélé au public et ne peut pas l'être. Dès lors, pour connaître leur fonctionnement intime, il faut procéder par expériences méthodiques et nombreuses. C'est pourquoi le Conseil national du numérique préconise la création « d'agences de notation pour mesurer les niveaux de neutralité » des plateformes. Il s'agit de :

Développer des agences de notation de la neutralité pour révéler les pratiques des plateformes et éclairer les usagers et partenaires dans leurs choix. Les doter de moyens d'enquête et d'observation pour les mettre en mesure de développer des indicateurs efficaces. Ces agences pourraient prendre plusieurs formes : publiques, privées, associatives ou basées sur la multitude (crowd) et la société civile»⁶⁰².

Un rapport du Conseil général de l'économie développe des propositions du même type : « Créer une plateforme collaborative scientifique, destinée à favoriser le développement d'outils logiciels et de méthodes de test d'algorithmes », mais aussi « Créer une cellule de contrôle spécialisée "bureau des technologies de contrôle de l'économie numérique", pour l'ensemble des pouvoirs publics, implantée au sein de la DGCCRF »⁶⁰³

Une deuxième direction, lorsque l'on cherche à rendre observables les biais dans la sélection d'information par les plateformes, est plus interventionniste. Elle oblige ces acteurs à proposer une information « non personnalisée ». Ainsi qu'il a déjà été exposé, tout réseau social est en mesure d'offrir à l'utilisateur une vue exhaustive et purement chronologique des publications opérées par ses contacts. Il devrait toujours être possible d'afficher cette vue. En revanche, un moteur de recherche n'a pas la possibilité de présenter des résultats « neutres », puisque toute sélection de sites

601. - Art. L. 111-7 C. conso. dans sa rédaction issue de la loi n° 2016-1321 précitée.

602. - CNNum, rapport *Neutralité des plateformes...*, précité, recommandation 2, p. 11.

603. - Conseil général de l'économie, *Modalités de régulation des algorithmes de traitement des contenus*, rapport de mai 2016, p. 41 et s.

opérée à partir d'une requête est une opération subjective⁶⁰⁴. Mais le moteur de recherche Google ne présente pas les mêmes résultats à un internaute identifié et à un « inconnu » - qui n'a pas de compte Google, et dont ni l'adresse IP, ni les cookies, ni aucune « trace » numérique ne permet de le rattacher à des habitudes passées. Chacun devrait pouvoir demander à être traité « comme un inconnu ». Cela permettrait aux utilisateurs, sans les y contraindre, de procéder par comparaison entre les résultats filtrés et les résultats bruts⁶⁰⁵. Ils verraient à l'œuvre les forces qui modèlent l'information dont ils sont consommateurs au quotidien. Libres à eux, ensuite, de retourner vers le confort d'un monde entièrement conçu à partir de leurs désirs, ou de dégonfler un peu la « bulle » de subjectivité qui les entoure, faute de pouvoir jamais la percer.

B - La véracité des contenus

174. « **Fake news** » et manipulations de masse - Un peu plus d'un mois avant son départ du pouvoir, M. Barack Obama a clairement affirmé que la Russie avait utilisé Internet pour peser sur le cours de l'élection présidentielle américaine. D'une part, des attaques informatiques auraient permis de dérober puis de laisser filtrer des informations sensibles concernant le Parti démocrate, et en particulier à sa candidate Hillary Clinton⁶⁰⁶. D'autre part, de fausses rumeurs, des informations mensongères patiemment diffusées des mois durant, auraient contribué à modeler lentement l'opinion publique américaine : les désormais célèbres *fake news*⁶⁰⁷. Une responsable du média russe *Sputnik* dévoile ainsi sa vision très particulière du journalisme : « *There are many different truths* », « *There has to be a pluralism of truth* »⁶⁰⁸. Cette dangereuse rhétorique des vérités multiples devait, croyait-on, rester cantonnée à quelques milieux interlopes. Mais l'élection de M. Donald Trump à la présidence des USA l'a convoquée directement dans les discours officiels de la plus grande démocratie du monde. Ainsi, le porte-parole de la Maison-Blanche avait affirmé, contre

604. - Lorsqu'un réseau social comme Facebook propose des suggestions — vous venez de lire tel article A proposé par l'un de vos contacts, vous aimerez probablement aussi les articles B et C —, on ne sait pas si ces suggestions seraient faites de la même manière à tout internaute ayant lu A, ou si elles sont personnalisées. Si elles sont personnalisées, il devrait être possible d'en obtenir une version non personnalisée.

605. - Pour faciliter cette comparaison, Mme Amal Taleb, vice-présidente du CNNum, proposait que le réseau social ou moteur de recherche affiche simultanément au moins deux onglets de résultats, l'un « personnalisé » et l'autre non (intervention au colloque « Le droit des personnelles », Amiens, 7 novembre 2016).

606. - V. par ex. E. Dvinina, « États-Unis : quelle riposte aux piratages russes ? », article *lemonde.fr* du 19 décembre 2016.

607. - Pour une étude universitaire de l'impact de ces fake news sur l'élection présidentielle américaine : H. Allcott et M. Gentzkow, « Social media and fake news in the 2016 election », *Journal of Economic Perspectives*, Volume 31, Number 2, Spring 2017, p.211-236, consultable sur le site de l'Université de Stanford : <https://web.stanford.edu/~gentzkow/research/fakenews.pdf>.

608. - A. Higgins, « It's France's turn to worry about election meddling by Russia », article *Nytimes.com* du 17 avril 2017.

toute évidence, que l'investiture avait mobilisé une foule sans aucun précédent historique. Interrogée sur ce mensonge, la conseillère Kellyanne Conway proposa une réponse qui restera dans les mémoires : « *[the press secretary] gave alternative facts* »⁶⁰⁹. Par la suite, le président retourna l'expression *fake news*, dont on aura compris qu'elle avait été forgée pour dénoncer les informations frelatées issues de sources douteuses, contre les médias traditionnels, affublant par exemple le vénérable New York Times de ce qualificatif. Le journal se défendit en diffusant un spot dont le mot d'ordre était : « *The truth is hard to find. The truth is hard to know. The truth is more important than ever* »⁶¹⁰. Ainsi M. Trump a-t-il légitimé un discours consistant à nier toute forme de hiérarchie entre les grands quotidiens d'investigation et les sites complotistes, entre les reporters professionnels et les blogueurs militants. Les citoyens sont encouragés à rechercher en ligne « les » vérités qui leur seraient cachées par les médias traditionnels. Les supports à privilégier seraient ceux qui n'ont ni la compétence, ni les moyens humains et financiers, ni même et surtout l'objectif de rechercher la vérité. Faits et opinions sont confondus ; la rotondité de la Terre devient un simple point de vue, et la science une croyance⁶¹¹. Internet, dont les utopistes imaginaient qu'il rendrait le savoir accessible à tous, abolit les frontières du vrai et du faux, fond certitudes et rumeurs dans son chaudron brûlant. Le risque de régression est réel. Des réponses juridiques peuvent-elles être envisagées ?

175. Le délit de diffusion de fausses nouvelles - À rebours des tendances qui viennent d'être exposées, le droit français distingue les opinions, qui sont libres et la prise de position sur la réalité d'un fait, qui est encadrée. Affirmer quelque chose d'objectivement faux ne suffit pas, bien heureusement, à encourir les foudres du droit pénal. Des conditions supplémentaires sont exigées pour que soit constitué l'un des délits dits « de fausses nouvelles »⁶¹². Le plus important d'entre eux, de par la généralité de son champ d'application, est prévu par la loi de 1881 sur la liberté de la presse :

*La publication, la diffusion ou la reproduction, par quelque moyen que ce soit, de nouvelles fausses, de pièces fabriquées, falsifiées ou mensongèrement attribuées à des tiers lorsque, faite de mauvaise foi, elle aura troublé la paix publique, ou aura été susceptible de la troubler, sera punie d'une amende de 45 000 euros*⁶¹³.

609. - Interview du 22 janvier 2017, sur laquelle V. par ex. A. Blake, « Kellyanne Conway says Donald Trump's team has "alternative facts"... », article *thewashingtonpost.com* du 22 janvier 2017.

610. - Vidéo « The truth is hard », 23 février 2017, sur la chaîne YouTube du New York Times.

611. - Sur ce dernier point : D. Larousserie, P. Barthélémy et C. Lesnes, « Après l'élection de Trump, la science entre en résistance », article *lemonde.fr* du 17 avril 2017.

612. - Sur l'ensemble de cette question, V. N. Deffains et J.-B. Thierry, « Fausses nouvelles » in *Rép. pén. Dalloz*, juillet 2015.

613. - Article 27 de la loi de 1881 précitée. Le deuxième alinéa ajoute : « Les mêmes faits seront punis de 135

D'autres incriminations sont sectorielles, tel ce texte Code électoral.

*Ceux qui, à l'aide de fausses nouvelles, bruits calomnieux ou autres manœuvres frauduleuses, auront surpris ou détourné des suffrages, déterminé un ou plusieurs électeurs à s'abstenir de voter, seront punis d'un emprisonnement d'un an et d'une amende de 15 000 euros*⁶¹⁴.

Dans tous les cas, la « nouvelle » doit s'entendre comme une « annonce d'un événement arrivé récemment, faite à quelqu'un qui n'en a pas encore connaissance »⁶¹⁵. Sont donc potentiellement concernées les pseudo-révélation mensongères portant sur une actualité, qui sont nombreuses chaque jour en ligne, mais pas « les commentaires, aussi choquants soient-ils, portant sur des faits antérieurement révélés »⁶¹⁶.

Les autres conditions d'application sont exigeantes. Les textes requièrent la démonstration d'un important trouble social : la paix publique doit avoir été touchée ou avoir été près de l'être dans un cas, et des suffrages doivent avoir été perdus ou détournés dans l'autre. Surtout, une véritable intention de nuire doit avoir animé celui qui a publié ou propagé la nouvelle. Le premier texte la réclame explicitement, qui vise la « mauvaise foi » ; le second, implicitement, qui fait allusion à des suffrages « surpris ou détournés », ce qui ne peut être le résultat que d'une manœuvre volontaire.

176. L'absence d'illicéité manifeste de l'acte de relais - Dès lors, il sera très difficile d'agir contre l'écrasante majorité des internautes, qui se seront contentés de relayer une fausse nouvelle à laquelle ils ont très bien pu croire. Nous avons vu que l'infraction de diffamation était constituée par la simple reproduction de propos attentatoires à l'honneur ou à la réputation : c'était ensuite à l'internaute d'exciper de sa bonne foi⁶¹⁷. Ici, c'est à l'accusation de démontrer la mauvaise foi. L'obstacle n'est certes pas insurmontable, mais comment l'infraction sera-t-elle utilisée, de fait ? Les autorités, avec le concours du réseau social qui a servi à la propager le cas échéant, tâcheront de remonter à l'origine des rumeurs, à ceux qui les ont fabriquées parce qu'ils y ont intérêt. Ce seront les instigateurs qui seront punis, et un petit nombre de relais du premier cercle dont on aura pu démontrer qu'ils partageaient leurs mauvais desseins. En revanche, l'écrasante masse des internautes aura souvent eu le seul tort d'être naïve ou crédule. Le résultat est que le partage d'une fausse nouvelle présentera rarement un caractère manifestement illicite. Or, nous avons vu que

000 euros d'amende, lorsque la publication, la diffusion ou la reproduction faite de mauvaise foi sera de nature à ébranler la discipline ou le moral des armées ou à entraver l'effort de guerre de la Nation ».

614. - Article L 97 du Code électoral. Sur les autres délits de fausses nouvelles : N. Deffains et J.-B. Thierry, art. préc., n° 5 s.

615. - CA Versailles, 4 février 1998, approuvée par Cass. crim., 13 avril 1999, n° 98-83.798.

616. - Même arrêt. De tels commentaires peuvent néanmoins tomber sous le coup d'une autre infraction, par exemple, au cas d'espèce, la diffamation.

617. - V.supra, n°142.

l'illicéité devait crever les yeux pour qu'un intermédiaire numérique puisse se voir reprocher d'être resté inerte après un signalement par un utilisateur⁶¹⁸.

Telle est en tout cas la situation du droit positif. Une proposition de loi avait envisagé de faire évoluer très nettement la situation des plateformes⁶¹⁹. Plusieurs nouveaux textes devaient place au sein du Code pénal, parmi lesquels celui-ci :

Art. 226-12-2. - Doit notamment être considéré de mauvaise foi, l'éditeur, le diffuseur, le reproducteur, le moteur de recherche ou le réseau social ayant maintenu à la disposition du public des nouvelles fausses non accompagnées des réserves nécessaires pendant plus de trois jours à compter de la réception du signalement par un tiers de leur caractère faux.

« L'éditeur, le diffuseur, le reproducteur, le moteur de recherche ou le réseau social à qui a été signalé le caractère faux des nouvelles peut néanmoins démontrer sa bonne foi en rapportant la preuve de l'accomplissement de démarches suffisantes et proportionnelles aux moyens dont il dispose afin de vérifier le contenu et l'origine de la publication mise à disposition.

Un seul signalement, réalisé par n'importe quel internaute, devait donc déclencher une enquête de la part d'un moteur de recherche ou réseau social. Le deuxième alinéa précisait cependant que les démarches devraient être « proportionnelles aux moyens dont il dispose ». Il est vrai que les ressources financières et humaines nécessaires pour procéder à des investigations complètes sur des milliers d'histoires douteuses sont potentiellement considérables. Sans ce deuxième alinéa, impossible d'imaginer un réseau social libre, décentralisé et à but non lucratif comme *Mastodon*⁶²⁰. Toutefois, la démarche « proportionnelle » semble difficilement compatible avec le principe de légalité des délits et des peines, tant il est difficile de déterminer *a priori*, pour un acteur donné, quel est le niveau de diligence attendu de sa part au regard de ses ressources. Laissons de côté cette objection, et raisonnons à partir de l'exemple des géants Facebook et Google, qu'on supposera dotés de moyens presque illimités. Même dans ce cas, le dispositif envisagé ne va pas sans susciter certaines réserves.

Cette proposition de loi semble devoir rester lettre morte. En revanche une proposition de loi relative à la lutte contre les fausses informations est débattue au moment où nous écrivons ces lignes, qui semble avoir de plus grandes chances d'être adoptée⁶²¹.

618. - V.supra, n°163.

619. - Proposition de loi n° 470 visant à définir et sanctionner les fausses nouvelles ou « fake news », déposée à la Présidence du Sénat par Mme Nathalie Goulet.

620. - Ce réseau est mis en œuvre notamment par des particuliers ou des associations, chacun utilisant son propre serveur.

621. - Proposition de loi n° 799 enregistrée le 21 mars 2018, relative à la lutte contre les fausses informations.

177. Facebook et Google, journalistes d'investigation ? - Le problème fondamental, s'agissant de ces fausses nouvelles, c'est que l'on attend des plateformes qu'elles pratiquent un métier qui n'est pas le leur. C'est une chose d'être chargé du retrait de contenus manifestement illicites, comme une négation de l'existence de la Shoah, ou l'appel à des violences contre un groupe d'individus caractérisé par son orientation sexuelle. C'en est une autre de procéder à des enquêtes pour démêler les actualités véritables des *fake news*. Dans le premier cas, il suffit de prendre connaissance de la publication pour connaître son devoir, qui est de la faire disparaître. Dans le second, il faudra mener des investigations, interroger des sources, procéder à des recoupements et des vérifications.

Nous rencontrerons d'autres exemples de cette tendance : celle qui voudrait traiter les nouveaux intermédiaires de l'économie numérique de la même façon que les acteurs anciens qu'elles ont partiellement évincés. Une plateforme de financement participatif permet aux internautes de se prêter de l'argent, sur la foi d'une description assez sommaire d'un projet industriel, artistique ou caritatif ? Il est tentant d'exiger de la plateforme qu'elle opère elle-même une sélection des projets les plus sérieux et qu'elle assume une responsabilité personnelle en cas d'échec, ce qui revient à terme à en faire... une banque, et à empêcher la multitude d'entrer en contact direct avec la multitude, ce qui était l'objectif initial. De la même façon, les réseaux sociaux ont permis aux utilisateurs de se retrouver en face les uns des autres par millions, l'intermédiaire se faisant le plus neutre et le plus discret possible. La tentation est grande de le ramener petit à petit vers un rôle de rédaction en chef, en exigeant de lui qu'il vérifie le contenu des discussions et qu'il distribue des mauvais points, le cas échéant. Il se voulait translucide, le voilà ramené vers la densité et la substance. Mais il ne faudrait pas oublier que sa déresponsabilisation n'est pas — totalement — artificielle : elle est une conséquence d'une modification véritable de son rôle. Le véritable rédacteur en chef assume professionnellement et juridiquement les publications d'une équipe délimitée, qu'il connaît. On demande ici aux intermédiaires numériques d'assurer le contrôle intellectuel d'une foule bigarrée et chaotique d'inconnus. Il serait sage de ne pas légiférer avant d'avoir pris le temps d'une réflexion sérieuse et construite sur les conséquences d'un tel modèle. Cela tombe bien : sans y être contraints — si ce n'est par la pression de l'opinion publique -, certains acteurs ont pris des initiatives qu'il sera bon d'observer avant d'agir.

178. Des initiatives récentes - Ne disposant pas en interne de toutes les forces nécessaires à la lutte contre la désinformation Google et Facebook ont, chacun à sa manière, décidé de faire appel à des forces extérieures.

L'approche récemment retenue par Google semble reposer sur le *crowdsourcing*, c'est-à-dire sur la sagesse du nombre. L'idée est de s'adresser à sa multitude de visiteurs pour signaler les contenus faux. Plutôt que de les retirer — ce qui impliquerait, pour l'entreprise, de procéder au préalable elle-même à une vérification complète de la véracité de l'information — elle dégradera progressivement la position des résultats de recherche ainsi dénoncés⁶²². C'est sur ce système que Wikipédia compte depuis longtemps pour éviter que les articles de l'encyclopédie ne se trouvent remplis de mensonges. L'un des cofondateurs du site vient d'ailleurs d'annoncer le lancement d'un nouveau média en ligne visant à « réparer » l'information, et basé lui aussi sur le *crowdsourcing*⁶²³.

Facebook, quant à lui, a décidé de sous-traiter les tâches de vérification à de grands médias traditionnels, dans le cadre d'un *Journalism Project*⁶²⁴. Pour la France, les noms du Monde, de l'école de journalisme de Sciences Po, de l'Express, de France info, de Libération, de 20 Minutes et de BFMTV sont ainsi cités. La rémunération qui leur sera versée est en cours de négociation. Les contenus faux verront leur visibilité dégradée ou seront assortis d'un avertissement au lecteur : « Si deux médias partenaires établissent que le contenu signalé est faux et proposent un lien qui en atteste, alors ce contenu apparaîtra aux utilisateurs avec un drapeau mentionnant que deux “fact-checkers” remettent en cause la véracité de cette information. Quand un utilisateur voudra partager ce contenu, une fenêtre s'ouvrira pour l'alerter »⁶²⁵. De plus, la publication ainsi marquée ne pourra pas servir de support à une exploitation publicitaire.

Si ces initiatives peuvent sembler louables, le risque d'une police privée des publications doit à nouveau être souligné, comme chaque fois qu'il est demandé aux plateformes d'agir sur des contenus qui ne sont ni manifestement illicites, ni objets d'une demande judiciaire de retrait⁶²⁶. Ce qui rassure, dans le projet actuel de Facebook, c'est qu'il repose sur un partenariat avec de véritables professionnels reconnus de l'information. Mais rien n'empêche cette entreprise de décider, plus tard, d'internaliser entièrement cette compétence, ce qui rendrait probablement son fonctionnement très opaque. Quant aux systèmes reposant sur la foule, comme celui de Google ou

622. - A. Grondin, « Google s'en remet aux internautes pour évacuer les “fake news” des recherches », articles *leschos.fr* du 26 avril 2017.

623. - W. Mérancourt, « Avec WikiTribune, un cofondateur de Wikipédia s'attaque aux “fake news” », article *letemps.ch* du 28 avril 2017.

624. - G. Pépin, « “Fake news” : Facebook va rémunérer des éditeurs français et fait sa publicité dans la presse », article *nextimpact.com* du 26 avril 2017.

625. - A. Delcambre, « Huit médias français s'allient à Facebook contre les “fake news” », article *lemonde.fr* du 06 février 2017.

626. - V. déjàsupra, n° 107 et n°163. En ce sens, L. Lessig : « Ce que Facebook est en train de développer, un système très sophistiqué d'identifier et d'isoler les fake news, c'est effrayant. L'idée qu'une entité privée puisse se livrer à ce genre de censure est toujours inquiétante » (M. Untersinger, « Lawrence Lessig : “Le problème de la démocratie actuellement c'est qu'elle n'est pas représentative” », article *lemonde.fr* du 23 avril 2017).

de Wikipédia, ils ne sont jamais à l'abri de manipulations à grande échelle, organisées par un acteur hostile. Pour se protéger contre la désinformation, le citoyen doit avant tout exercer son esprit critique, savoir croiser et hiérarchiser les sources, toutes choses qui s'enseignent mieux qu'elles ne se décrètent.

LA COMMUNICATION NUMÉRIQUE : CONCLUSION

C'est la vocation d'Internet que de permettre une « conversation mondiale sans fin », facile et bon marché. Le réseau s'impose progressivement comme le principal moyen de recevoir, mais aussi d'adresser de l'information. Les facultés d'y accéder et de s'y déplacer librement ont alors logiquement été consacrées comme des libertés fondamentales, qui ne peuvent recevoir que des limitations justifiées et proportionnées.

Les médias pré-numériques étaient conçus de manière essentiellement pyramidale : un petit nombre de plumes et de voix interpellait la multitude. Mais le nouveau schéma est une nébuleuse : tout internaute dispose des moyens de prendre la parole, de répondre et de contredire. Chacun peut s'adresser à tous. Les règles relatives à la liberté d'expression doivent-elles évoluer en conséquence ? Certains aspects du discours numérique se laissent facilement saisir par les schémas anciens, mais pas tous. En particulier, la possibilité offerte par les nouveaux médias de se faire le relais d'autrui — par la pose de liens hypertextes, par des boutons de partage ou l'expression « d'émotions » face à un contenu — n'est pas sans poser de délicates questions. Il a fallu se demander par ailleurs si les courtes prescriptions typiques du droit de la presse, imaginées pour le papier, étaient adaptées aux supports électroniques. Nous avons conclu que la plupart de ces difficultés se passaient de réglementations véritablement nouvelles, et n'appelaient que des ajustements ponctuels – les responsables publics devraient se méfier, en la matière, des intuitions et des réactions à vif.

En revanche, force est de constater que les cadres anciens sont malhabiles à saisir le rôle des plateformes de communication, parmi lesquelles les réseaux sociaux occupent une place de choix. Ces acteurs jouent un rôle nouveau, qui ne connaît pas de strict équivalent dans le monde hors-ligne. Ils ouvrent leurs colonnes virtuelles à leurs utilisateurs, sans pour autant assurer une rédaction en chef ni plus largement de contrôle *a priori* sur les publications. C'est grâce à eux ou à cause d'eux que l'information se propage, mais il est irréaliste de les tenir pour comptables, de manière inconditionnelle et systématique, des abus de la liberté d'expression commis dans l'utilisation de leurs services. Un équilibre délicat doit être trouvé entre la faible responsabilité qu'appelle

naturellement leur statut d'intermédiaire technique, et la nécessité de lutter contre les discours de haine. La tentation de faire peser sur eux des obligations renforcées contient en germe un risque de dérapage très inquiétant : l'émergence d'une véritable censure privée, qui serait d'autant plus impitoyable qu'elle prendrait des risques importants en se montrant laxiste, mais ne s'exposerait à aucun danger en cas d'excès de zèle.

La question de leur statut se révèle d'autant plus délicate si l'on dépasse la seule question de leur inertie supposée face aux propos les plus violents, et que l'on s'interroge sur leurs responsabilités en matière d'agencement de l'information. En effet, ces plateformes ne se contentent pas de relayer de manière neutre et exhaustive les contenus proposés par les utilisateurs : à l'aide d'algorithmes, elles les filtrent pour complaire à ceux qui compulsent leurs fils d'actualité, au risque d'offrir aux internautes une vision excessivement personnalisée, et donc biaisée, du monde qui les entoure. Ce n'est pas tout : les controverses récentes relatives au rôle supposé des *fake news* dans les campagnes électorales à travers la planète ont fait pression sur ces sociétés, qui prétendent à présent tenir compte de la véracité supposée des publications dans la manière de les valoriser ou de les marginaliser. Finalement, une rédaction en chef d'un nouveau genre se profile, dont les ressorts seront occultes, et les résultats variables pour chaque utilisateur. À l'heure où les réseaux sociaux se positionnent comme la première source d'information d'un grand nombre d'individus, ces évolutions interpellent nécessairement le juriste.

Deuxième notion - La propriété

179. **Un concept en mouvement** - « La propriété est le droit de jouir et disposer des choses de la manière la plus absolue, pourvu qu'on n'en fasse pas un usage prohibé par les lois ou par les règlements ». La définition figurant à l'article 544 du Code civil impressionne par sa vigueur et rassure par sa concision. Mais rarement simplicité aura été aussi trompeuse. Le concept ploie sous la charge politique, philosophique, économique qui lui est associée. Son contenu exact a varié et son unité s'est fissurée, au fil d'une histoire complexe que cette étude n'a pas pour objet de retracer, mais plus modestement d'illustrer, et de confronter aux technologies numériques¹. Une esquisse sera rapidement réalisée à grands traits.

Pour comprendre quelle conception de la propriété avait été retenue par les rédacteurs du Code Napoléon, il est nécessaire de rappeler qu'elle a été construite par réaction à l'Ancien droit. La propriété immobilière, la seule qui importait véritablement alors, y était systématiquement fragmentée. « Par exemple, dans une même forêt, l'un pouvait avoir droit aux taillis, l'autre aux arbres de haute futaie ; dans une prairie, l'un pouvait avoir droit aux premières herbes, l'autre aux regains ; dans un étang, l'un avait droit aux poissons quand il était en eau, l'autre à la culture quand il était à sec »². Mais le démembrement le plus connu et le plus important était celui entre « domaine utile » — dévolu à ceux qui exploitaient la terre, temporaire — et « domaine éminent » — conservé par le seigneur, qui était rémunéré pour l'utilisation de la terre et en contrôlait les actes de disposition³. Ainsi le propriétaire « utile » était-il soumis à une tutelle aliénante et ruineuse. C'est pour conjurer ces démons et émanciper les individus que la Révolution instaura un droit de propriété absolu, exclusif et perpétuel. La seconde partie de l'article 544 du Code civil, qui nuance ce caractère égoïste, aurait été largement ignorée au cours du XIXe siècle⁴. Il faut enfin rappeler que

1. - On se reportera à la bibliographie recensée par J. Rochfeld, *Les grandes notions...*, *op. cit.*, n° 5.32 et s.

2. - P. Malaurie et L. Aynès, *Les biens*, Defrénois, 5e éd., 2013, n° 406.

3. - F. Terré et P. Simler, *Droit civil. Les biens*, Dalloz, 9e éd., 2014, n° 79.

4. - J. Rochfeld, *Les grandes notions...*, *op. cit.*, n° 5.12 : « Il fallait, rappelons-le, marquer une franche rupture par rapport à la situation antérieure et un rejet net de la renaissance des charges féodales (...). IL le fallait d'autant que le XVIIIe siècle avait installé l'idée que les droits individuels devaient prendre une forme absolue. La propriété conçue comme le reflet de la liberté individuelle ne pouvait donc souffrir aucune atteinte au droit du propriétaire, de sorte que sa composante sociale fut minimisée ». Comp. C. Atias, *Droit civil. Les biens*, Lexisnexis, 12e éd., 2014, n° 122, qui met en garde contre une « illusion d'ordre positif et historique » : « [...] la propriété illimitée ne résulte pas des textes actuels — c'est l'évidence -, mais elle ne ressortait pas davantage du Code civil qui n'avait rien de libéral ».

ce tête-à-tête entre le propriétaire et son bien avait été pensé pour le monde des choses corporelles, la domination du premier sur la seconde se traduisant par une emprise physique sur la matière⁵.

Individualisme et matérialité : ces deux piliers de la propriété de 1804 ont été depuis lors largement ébranlés. Le mouvement est général, mais le numérique en fournira de frappantes illustrations.

180. Le recul de l'individualisme - Un mouvement de « réintégration des tiers » s'est engagé à la fin du XIXe siècle, sous l'influence notamment des théories de Planiol, Duguit et Josserand⁶. Le premier imagine une « obligation passive universelle » pesant sur tous les membres de la société, qui leur commande de respecter la situation créée par l'existence de la propriété⁷. En un sens, c'est déjà rétablir une relation aux autres que d'exiger d'eux qu'ils passent leur chemin. Le deuxième va bien plus loin : « le propriétaire ne serait pas légitime à utiliser sa chose dans un intérêt purement égoïste, mais devrait s'en servir conformément au bien de la collectivité »⁸. Ce n'est pas un droit qui est exercé, mais une fonction sociale⁹. Josserand est un peu plus mesuré, qui continue à considérer la propriété comme un droit, mais il affirme qu'en faire un usage socialement néfaste constitue un abus passible de sanction¹⁰. En droit positif, le propriétaire doit ainsi courber l'échine face à de multiples réglementations destinées à assurer la primauté de l'intérêt général en matière d'urbanisme, d'environnement, de patrimoine. Il peut subir des servitudes d'utilité publique, être exproprié. Il y a quelques années, le Tribunal de l'Union européenne a pu résumer la situation ainsi :

(...) si le droit de propriété et le libre exercice d'une activité économique font partie des principes généraux du droit communautaire, ces principes n'apparaissent pas pour autant comme des prérogatives absolues, mais doivent être pris en considération par rapport à leur fonction dans la société. Par conséquent, des restrictions peuvent être apportées à l'usage du droit de propriété et au libre exercice d'une activité professionnelle, à condition que ces restrictions répondent effectivement à des objectifs d'intérêt général poursuivis par la Communauté et ne constituent pas, au regard du but recherché, une intervention démesurée et intolérable qui porterait atteinte à la substance même des droits ainsi garantis (...)¹¹.

5. - *Ibid.*, n° 5.4.

6. - J. Rochfeld, *Les grandes notions...*, op. cit., n° 5.12.

7. - M. Planiol, *Traité élémentaire de droit civil conforme au programme officiel des facultés de droit. Tome 1, Principes généraux, les personnes, la famille, les incapables, les biens*, LGDJ, 5e éd., 1908.

8. - La théorie de Duguit est ainsi décrite par W. Dross, *Droit des biens*, LGDJ, 2e éd., 2014, n° 37.

9. - L. Duguit, *Les transformations générales du droit privé depuis le Code Napoléon*, éd. F. Alcan, 2e éd., 1920.

10. - L. Josserand, *De l'esprit des droits et de leur relativité : théorie dite de l'abus des droits*, Dalloz, 1939.

11. - Tribunal de l'UE, 2 mars 2010, T-16/04, *Arcelor SA c./ Parlement européen*, § 153.

Cette tension entre pouvoir absolu du propriétaire sur son bien et nécessité de tenir compte de l'intérêt général trouvera à s'illustrer en droit du numérique. À titre d'exemple, nous verrons que l'Europe et les USA sont en train d'adopter une attitude très différente face aux propriétaires de réseaux de communication. Les laisser libres d'agir à leur guise est susceptible de compromettre profondément le bon fonctionnement du réseau des réseaux.

Par ailleurs, certains ne souhaitent pas se contenter d'une « socialisation » plus importante du droit de propriété : ils considèrent que l'appropriation privée devrait être, en certains domaines, rejetée dans son principe même. Ces biens sont qualifiés de *Commons*, ou communs, dans la lignée des travaux de l'économiste américaine Elinor Ostrom¹². Ils ont fait l'objet d'un regain d'intérêt ces dernières années¹³. L'objectif est la mise en place de règles de gestion permettant la préservation d'une ressource d'intérêt général dans un temps long, associée à la mise à disposition de ses utilités au plus grand nombre. Les communs sont invoqués dans le domaine des choses tangibles, par exemple en matière d'environnement¹⁴. Mais ils sont également recherchés dans le domaine de l'immatériel, pour favoriser notamment la circulation du savoir¹⁵. Or, l'histoire de la création d'Internet que nous avons brièvement abordée en introduction de cette étude, doit beaucoup à des groupes de chercheurs et d'ingénieurs très sensibles à la collaboration désintéressée, ainsi qu'à la circulation gratuite des idées¹⁶.

181. Le recul du matérialisme - Les choses matérielles, il vient d'en être question, ne constituent plus les seules richesses, ni même les plus considérables. Certaines valeurs, auparavant tangibles, ont perdu peu à peu leur *corpus*, comme les titres de société, ou l'argent lui-même. D'autres n'en ont jamais eu : le fonds de commerce, l'œuvre de l'esprit. Le pouvoir sur de tels actifs ne peut s'exercer selon les mêmes modalités. Le propriétaire peut se tenir debout sur son fonds et y bâtir ; il peut enfermer ses lingots dans un coffre ou brûler ses titres au porteur. Sa puissance s'exercera différemment sur les nombreux actifs incorporels mobilisés par le monde du numérique, au premier rang desquels les œuvres de l'esprit. « Il n'y a plus de possesseurs, mais que des créanciers »¹⁷. La propriété immatérielle est-elle encore la propriété ? Pour M. Gutmann, ce ne peut

12. - Not. E. Ostrom, *Gouvernance des biens communs : pour une nouvelle approche des ressources naturelles*, trad. L. Baechler, De Boeck, 2010.

13. - B. Coriat (dir.), *Le retour des communs : la crise de l'idéologie propriétaire*, Les liens qui libèrent, 2015.

14. - E. Ostrom, *op. cit.* ; A. Chaigneau, (dir.), *Fonctions de la propriété et communs. Regards comparatistes*, Société de législation comparée, vol. 27, 2017.

15. - L. Lessig, *L'avenir des idées*, trad. française de J.-B. Soufron et A. Bony, Presses Universitaires de Lyon, 2005 ; H. Le Crosnier, *En communs : une introduction aux communs de la connaissance*, C&F éditions, 2015.

16. - V.*supra*, n°10.

17. - E. Lévy, *Les fondements du droit*, Paris, 1922, cité par F. Zénati, « L'immatériel et les choses », in *Le droit et l'immatériel*, *Archives de philosophie du droit*, t. 43, p. 79.

être qu'au prix d'analogies incessantes entre les concepts applicables au monde perceptible et ceux qui règnent dans l'éther, ce qui aboutira à une distorsion des notions finalement nuisible. L'auteur s'amuse d'un attendu imaginaire pour illustrer son propos, dans un domaine qui nous concerne au premier chef : « Attendu que s'il est permis de surfer librement sur les autoroutes de l'information, les navigateurs sont tenus de respecter les défenses anti-invasion d'autrui »¹⁸. Puis il dénonce un raisonnement en forme de cercle vicieux :

*(...) puisque les réalités immatérielles ont de la valeur, il est inévitable qu'elles soient appréhendées par le droit ; il faut donc qu'elles soient des biens, puisqu'à l'exception des personnes morales, ces réalités immatérielles ne sont pas des personnes ; et puisqu'il faut qu'elles soient des biens, il faut nécessairement qu'elles soient appropriables. Voici le vice fondamental de l'enchaînement : pour donner prise au droit, les réalités immatérielles sont autoritairement encadrées par l'a priori du bien et de la propriété*¹⁹.

D'autres auteurs, à l'inverse, considèrent que la préoccupation du droit des biens a toujours été la protection d'une « valeur », qui s'accommode fort bien de l'absence de *corpus*²⁰. D'autres encore estiment que l'immatériel n'est bien souvent qu'une illusion, et qu'un *corpus*, certes plus discret, peut y être discerné²¹.

Le numérique fournira de nombreux exemples de situations dans lesquelles la valeur d'une chose immatérielle fait l'objet d'une réservation. Nous verrons si ses modalités semblent compatibles avec le concept de propriété.

182. À qui Internet appartient-il ? - Toutes les évolutions, tensions et incertitudes qui animent le droit de propriété se rencontrent sur la scène numérique. Nous avons vu que la propriété privée, dans son acception la plus classique, constitue un droit de jouir seul et absolument de sa chose. Elle est un pouvoir d'exclure autrui. À ce titre, elle est parfois considérée comme un ennemi par les défenseurs d'un Internet qui s'est historiquement bâti sur une large mutualisation des connaissances et des ressources. Mais le réseau global est aussi le lieu d'investissements immenses en argent, en temps et en compétences, qui ne sont pas tous désintéressés. Des industries y prospèrent, parmi les plus puissantes du monde moderne. Elles y accumulent un capital, auquel il sera donné accès par le jeu de contrats, mais qui peut s'analyser avant cela sous l'angle des droits réels. En somme, sur

18. - D. Gutmann, « Du matériel à l'immatériel dans le droit des biens. Les ressources du langage juridique », in *Le droit et l'immatériel, Archives de philosophie du droit*, t. 43, p. 65.

19. - *Ibid.*

20. - F. Zénati, « L'immatériel et les choses », art. préc.

21. - P. Catala, « L'immatériel et la propriété », in *Le droit et l'immatériel, Archives de philosophie du droit*, t. 43, p. 63 : « (...) la physique a débusqué les micro-éléments constitutifs de l'énergie et l'on sait aujourd'hui que les rayons sillonnant l'espace sont à la fois des ondes et des flux de particules. Où se situe désormais l'immatériel ? ».

Internet, coexistent des communautés qui s'appuient sur l'immatérialité et la non-rivalité pour repousser autant que possible le recours à la propriété privée, et les titans du capitalisme contemporain, dont la propriété constitue le cœur battant.

Encore faut-il préciser qu'« Internet » est un concept-monde qui mêle, dans le discours public, un ensemble complexe de protocoles, d'équipements, de machines et d'idées. Le mot désigne des tuyaux, ce qui en coule et comment l'on s'en sert. Cet ensemble doit être déconstruit, sous peine d'être impossible à manipuler. L'un des premiers juristes à se livrer à cet exercice, le professeur américain Yochai Benkler, identifie trois « couches » : « *the physical infrastructure layer - wires, cable, radio frequency spectrum - the logical infrastructure layer - software - and the content layer* »²². D'autres présentations sont évidemment possibles, selon ce que l'observateur cherche à étudier ou à mettre en évidence²³. Nous retiendrons un schéma très proche, envisageant Internet comme un ensemble d'infrastructures matérielles et logicielles (section 1) qui véhiculent des contenus (section 2) consultables à l'aide de terminaux (section 3).

Section 1 - Les infrastructures

183. **Plan** – Internet est avant tout un gigantesque agglomérat de réseaux de télécommunications, conçu de manière décentralisée (I). Des parties peuvent en être retranchées ou y être ajoutées régulièrement, sans aucun dommage pour le fonctionnement général. Mais l'on peut toutefois identifier par ailleurs une tête, ou un cœur. Il s'agit du grand annuaire mondial des adresses IP et des noms de domaine, une structure de coordination à l'échelle mondiale (II).

22. - Y. Benkler, « From Consumers to Users: Shifting the Deeper Structures of Regulation Toward Sustainable Commons and User Access », *Federal Communications Law Journal*, 200, vol. 52: Iss. 3, Article 9. Article consultable à l'adresse : <http://www.repository.law.indiana.edu/fclj/vol52/iss3/9>. Cette classification sera reprise par L. Lessig, dans ses différents ouvrages cités.

23. - J.-C. Guédon, préface à L. Lessig, *L'avenir des idées*, op. cit. : « [...] tout système de communication peut se comprendre comme un système en “couches”, à l'instar des réseaux comme l'Internet. Les ingénieurs de l'Union Internationale des Télécommunications ont ainsi développé un modèle (OSI) en sept couches qui paraît devoir se limiter à jouer le rôle d'enveloppe théorique des réalisations techniques réelles ; pour leur part, les ingénieurs de l'Internet se sont contentés de quatre couches. Benkler simplifie encore plus l'analyse générale des systèmes de communication en ne conservant que trois couches : une couche “physique” à travers laquelle la communication s'effectue physiquement (le cuivre des lignes téléphoniques classiques, la fibre optique des réseaux actuels), une couche logique qui permet à la “quincaillerie” de fonctionner — les protocoles de l'Internet correspondent à ce niveau que Lessig appelle aussi le “code” —, enfin une couche de “contenu”, c'est-à-dire les messages eux-mêmes qui circulent dans nos sociétés. Dans le monde de l'imprimé, le papier et l'encre correspondraient à la première couche ; le format du papier, le choix de la langue, la typographie et la mise en page à la deuxième couche ; les articles eux-mêmes avec leur signification propre à la troisième couche ».

I – La télécommunication

184. **Un tout plus grand que ses parties** – Dans la classification proposée par M. Benkler, les infrastructures de communication renvoient à la fois à la couche « physique » d’Internet et à sa couche « logique ».

La couche matérielle consiste en une variété d’équipements, certains lourdement tangibles — fibres optiques sous-marines et terrestres, millions de kilomètres de câbles de cuivres, routeurs — d’autres à la matérialité plus éthérée : réseaux wifi ou de téléphonie mobile, liaisons satellites par exemple. Historiquement, le réseau militaire ARPANET a constitué le *backbone*, l’épine dorsale des infrastructures. Aujourd’hui, il n’existe plus de réseau central qui s’opposerait de manière officielle à un réseau périphérique, mais certaines sociétés peuvent être considérées, par la taille et le débit exceptionnels de leur réseau de communications, comme constituant de fait un noyau à l’échelle mondiale. La plupart de ces sociétés sont américaines : *American Telephone & Telegraphy Company* (AT&T) en constitue l’exemple le plus illustre²⁴. Une société européenne, aujourd’hui disparue avait affiché son ambition d’intégrer cette épine dorsale en prenant le nom d’*Ebone*, pour *European Backbone*²⁵. À ces grands fournisseurs d’accès se connectent ensuite des propriétaires de réseaux plus petits, qui développent leur propre clientèle. Les FAI français entrent essentiellement dans cette catégorie. Enfin, les abonnés constituent parfois leur propre réseau domestique ou d’entreprise, qui peut être considéré comme partie intégrante du réseau global. C’est ce dernier maillon qui se prête à l’exercice le plus puissant du droit de propriété, car, au premier abord, seul son titulaire en subira les conséquences. Cette impression doit être nuancée : il a déjà été exposé que la loi française fait peser sur chacun une obligation de veiller à la sécurité de sa connexion, afin d’éviter que son réseau ne soit exploité par un tiers se livrant à des actes de contrefaçon²⁶. Au-delà de cette disposition spécifique relevant du droit d’auteur, il est possible d’imaginer qu’une négligence coupable dans la sécurisation d’un réseau privé pourrait être une source de responsabilité civile, par exemple si les machines compromises ont été utilisées pour mener une cyberattaque. Il y aurait, en quelque sorte, une obligation — sans doute de moyens — de veiller à ce que son réseau ne soit pas utilisé pour nuire à autrui, mais pas davantage. Laissons de côté ce dernier maillon dans la chaîne de communication, et considérons les infrastructures des petits et

24. - Sont souvent cités les noms de UUNET, Level 3, Verizon, AT&T, Qwest, Sprint et IBM (v. par ex. <http://computer.howstuffworks.com/internet/basics/who-owns-internet1.htm>). Sur le rôle central joué par AT&T dans l’histoire d’Internet, V. L. Lessig, *L’avenir des idées*, op. cit., première partie, chapitre 2.

25. - E. Haroff, « France Telecom opens European Backbone Network », article *lightwaveonline.com* du 1^{er} février 2000.

26. - V.supra, n°51.

grands FAI. La manière dont elles sont gérées est susceptible d'avoir un impact sur le fonctionnement d'Internet. Si le propriétaire d'un morceau de réseau, par lequel transitent des communications du monde entier, peut refuser de relayer certaines informations, ou est autorisé à les ralentir ou à les altérer, les fonctionnalités collectives s'en trouvent atteintes. Une tension se révèle entre le pouvoir exclusif d'une personne sur sa chose, et l'intérêt général.

Cette considération amène naturellement à décrire la couche logique, car elle pilote la couche matérielle, elle lui fournit ses instructions. Il s'agit en particulier de l'ensemble de protocoles appelé TCP/IP. Pour que l'interconnexion des réseaux privés soit possible, il est nécessaire que ces protocoles soient utilisés partout. Or, nous verrons qu'ils ont été originellement conçus de sorte à réduire au maximum la capacité du propriétaire du réseau à discriminer selon les différents flux qui transitent par ses équipements.

De ce qui précède découle un paradoxe apparent ainsi résumé par M. Lessig :

Internet est un réseau de réseaux. Pour dire les choses simplement, ces réseaux sont connectés entre eux par des câbles. Tous ces câbles et les machines qui y sont reliées sont sous le contrôle de quelqu'un. Il s'agit presque toujours de personnes privées : en d'autres termes, ils appartiennent à des individus ou à des entreprises qui ont décidé de se relier au Net. Certains sont la propriété de l'État. Pourtant, c'est ce vaste réseau de technologie privée qui a permis la mise en place d'un des plus importants biens communs de l'innovation que nous ayons jamais connus. Construits sur une plateforme réglementée, les protocoles d'Internet ont ouvert un espace libre propice à l'innovation. Ces réseaux privés ont créé une ressource ouverte dont tout un chacun peut retirer quelque chose, et que beaucoup ont déjà utilisée avec profit²⁷.

Un agglomérat de propriétés privées formant une ressource commune : l'histoire est belle. Elle l'est sans doute trop. La tentation existe, aujourd'hui, chez les propriétaires de réseaux, de brandir plus fermement leurs prérogatives pour modifier la manière dont les informations voyagent l'Internet global (A). Le bien commun des origines se trouve alors menacé de fragmentation et d'enclosure²⁸. Certains États ont alors décidé d'imposer le retour à « l'état de nature » qu'est la neutralité du net, mais ils se présentent sur ce front en ordre dispersé (B).

A – La tentation privée : discriminer les flux

185. **Plan** – Hasard ou volonté ? Les pères fondateurs d'Internet l'avaient conçu de manière à ce que les informations, toutes les informations, bénéficient d'un égal accès aux infrastructures de transport (1). Depuis quelques années, cette philosophie est largement menacée (2).

27. - L. Lessig, *L'avenir des idées*, op. cit., première partie, chapitre 2.

28. - A. Chaigneau, « Propriété et souveraineté de l'Internet : la maîtrise d'une infrastructure », in *Les biens numériques*, éd. Cepisca, 2015, p. 18.

1. – La neutralité des origines

186. **Le choix d'une architecture *end-to-end*** - Souvent considéré comme la matrice de la neutralité du net, le principe « end-to-end » a été formalisé de manière particulièrement claire dans un article publié en 1984 par des chercheurs du M.I.T²⁹. Il permet de comprendre quelle philosophie anime les protocoles TCP/IP. La question centrale explorée par les chercheurs est celle-ci : les réseaux de télécommunications doivent-ils être conçus de sorte à non seulement transporter l'information, mais aussi à en assurer par eux-mêmes un traitement ? Ou faut-il considérer que le réseau doit être essentiellement cantonné à sa fonction de véhicule, et laisser les logiciels s'exécutant aux extrémités de la chaîne seuls maîtres du traitement ? Pour le savoir, les auteurs examinent plusieurs exemples de « fonctions » qui pourraient être confiées soit au réseau de transport, soit aux bouts de chaîne, soit aux deux, puis ils recherchent la méthode la plus pragmatique et la plus efficace.

La première fonction étudiée est celle qui consiste à vérifier qu'un fichier a été transmis depuis le disque dur d'un ordinateur A jusqu'au disque dur d'un ordinateur B, séparés par le réseau de télécommunication, sans avoir été endommagé d'aucune manière. Cette fonction de vérification d'intégrité peut être conférée aux nœuds du système de transport de l'information : à chaque « saut » entre deux points du réseau, il est vérifié que la consistance du fichier n'a pas varié. La solution peut sembler logique au premier abord : le réseau est faillible, il peut dysfonctionner et perdre des informations. Pourtant, elle est à proscrire, car le fichier a également pu être corrompu en amont ou en aval. L'ordinateur A peut avoir mal lu le fichier sur son disque dur, l'avoir mal retranscrit dans sa mémoire, ou l'avoir mal transféré vers son module de communication externe. L'ordinateur B, qui exécutera les mêmes opérations dans l'ordre inverse, est exposé aux mêmes risques. Il n'est donc pas possible d'éviter que l'ordinateur B, à l'issue de la communication, compare le fichier qui lui a été transmis à l'empreinte qui l'accompagnait, et vérifie qu'il y a correspondance : c'est le seul moyen de valider l'ensemble des opérations de transfert, aussi bien celles qui dépendent du réseau que celles qui n'ont rien à voir avec lui. La conclusion est la suivante : demander aux nœuds du réseau d'effectuer ce travail est inutile, puisque le logiciel situé en bout de chaîne devra l'accomplir quoiqu'il arrive. La meilleure solution, la plus économe en ressources, la plus rapide, la plus efficace est de transporter servilement les paquets, quitte à recommencer l'envoi si quelque chose s'est mal passé à un quelconque niveau.

29. - J.H. Saltzer, D. P. Reed et D. D. Clark, « End-to-end arguments in system design », *ACM Transactions on Computer Systems*, vol. 2, issue 4, nov. 1984, p. 277, consultable en ligne : <http://web.mit.edu/Saltzer/www/publications/endtoend/endtoend.txt>.

Parmi les autres exemples de fonctions étudiés, figure celui du chiffrement. Il a déjà été évoqué dans cette étude : seul un chiffrement *end-to-end* procure un degré de sécurité satisfaisant³⁰. Si c'est le réseau de communication qui est chargé de rendre les données illisibles pour éviter leur compromission en cas d'écoute par un tiers, il sera toujours possible d'intercepter des données en clair entre le terminal A et le réseau, ainsi qu'entre le réseau et le terminal B. C'est à nouveau aux logiciels exécutés aux bouts de la chaîne qu'il revient d'accomplir cette tâche de traitement de l'information.

Un autre exemple de fonction est celui du *first-in, first-out* (FIFO), qui vérifie qu'un ensemble de messages échangés entre des parties arrive dans le même ordre que celui dans lequel ils ont été envoyés. Les différents paquets ont pu voyager en empruntant des chemins différents sur le réseau. Seuls les bouts de chaîne ont une vision d'ensemble de la discussion, et sont capables d'assurer cette mise en ordre.

Le dernier exemple qui peut être pris parmi ceux développés par les auteurs, et peut-être le plus frappant, est celui des conversations en temps réel. Chacun en a déjà fait l'expérience : lors d'une telle discussion, surtout lorsqu'elle combine de la vidéo à la voix, le signal est parfois dégradé. Cela s'explique par le fait que, lorsque des paquets sont perdus ou corrompus, les applications de *chat* font le choix de ne pas demander leur renvoi systématique. Appliquer une telle politique introduirait un temps de latence important, qui rendrait l'échange désagréable, voire impossible. Il est généralement possible de comprendre un correspondant si une faible fraction du signal sonore ou vidéo disparaît. En revanche, expliquent les auteurs, s'il s'agit de laisser à une autre personne l'équivalent d'un message répondeur, l'exigence d'un faible temps de latence disparaît, tandis que l'exigence de fiabilité est renforcée - il n'est pas possible de demander à son interlocuteur de répéter le message si un mot est inaudible. Le logiciel procèdera donc à un arbitrage différent et demandera donc beaucoup plus facilement que des paquets d'information lui soient renvoyés. La démonstration est faite, magistralement, que ces décisions ne peuvent être prises par le réseau, mais uniquement *end-to-end*, d'un bout à l'autre de la chaîne.

187. Un choix propice à l'innovation - Le choix du *end-to-end* apparaît donc avant tout comme de raison, mais présente de surcroît l'avantage d'offrir une plasticité maximale à Internet pour l'avenir. Ainsi l'un des auteurs de l'article a-t-il déclaré plus tard :

Nous voulions nous assurer que nous n'avions pas au bout du compte bâti une technologie réseau sous-tendue par une infrastructure [...] qui nous empêcherait d'intégrer une autre infrastructure de transport qui se serait révélée intéressante dans le futur. [...] Telle est la vraie raison pour laquelle nous avons opté pour cet outil d'une

30. - V.supra, n°85.

extrême simplicité appelé le protocole Internet³¹.

Mais c'est M. Lessig qui décrit le mieux les conséquences politiques, au sens large, d'un choix architectural qui pouvait sembler éminemment technique.

Cette structure a d'importantes conséquences pour ce qui est de l'innovation. On peut en compter trois :

Premièrement, parce que les applications fonctionnent sur des ordinateurs qui sont aux « bouts » du réseau, les inventeurs qui mettent au point de nouvelles applications ont seulement besoin de connecter leur ordinateur au réseau pour les faire fonctionner. Aucune modification des ordinateurs situés dans le réseau n'est nécessaire. Par exemple, si vous êtes un inventeur et que vous souhaitez pouvoir utiliser Internet pour passer des appels téléphoniques, il vous suffit de mettre au point un logiciel adéquat et de pousser les usagers à l'utiliser pour qu'Internet devienne capable de faire passer des appels téléphoniques. Vous pouvez écrire le programme et l'envoyer à une personne à l'autre bout du réseau. Vous l'installez tous les deux et vous pouvez vous mettre à parler. C'est tout.

Deuxièmement, parce que sa structure n'est optimisée pour aucune application existante spécifique, le réseau est ouvert à toute innovation non prévue à l'origine. Tout ce que fait le protocole Internet (IP), c'est de trouver le moyen de rassembler et faire circuler les données, il ne dirige ni ne traite certains types de données plus favorablement que d'autres. Cela crée un problème pour certaines applications [...], mais cela laisse aussi toutes leurs chances à une large palette d'autres applications. Ce qui veut dire que le réseau est ouvert à l'arrivée d'applications qui n'avaient pas été originellement programmées par ses créateurs.

Troisièmement, parce que la structure est celle d'une plate-forme neutre — « neutre » en ce sens que le propriétaire du réseau ne peut sélectionner certains « paquets » de données au détriment de certains autres — le réseau ne peut pas exercer de discrimination contre une nouvelle structure innovante. Si une nouvelle application menace une application en situation dominante, le réseau ne peut rien y faire. Quelle que soit l'application, le réseau restera neutre.

Le réseau est donc constitué de « tuyaux idiots » (*dumb pipes*), qui doivent simplement faire leurs « meilleurs efforts » pour acheminer les paquets d'information, sans considération aucune pour leur contenu, selon le principe « premier arrivé, premier servi » : cela revient à décrire la neutralité du net³². Ces solutions ont des vertus considérables à l'échelle collective, mais elles diminuent singulièrement les pouvoirs que les bâtisseurs de réseaux de communication pouvaient espérer tirer de leur propriété privée. Elles ont donc été combattues par certains opérateurs.

31. - Entretien téléphonique de David P. Reed avec Lawrence Lessig datant du 7 décembre 2001, cité par L. Lessig, *L'avenir des idées*, op. cit., première partie, chapitre 2, V. note 87.

32. - J. Cattan, « La protection de la neutralité de l'Internet : pour un accès neutre aux biens numériques » in *Les biens numériques*, éd. Ceprisca, 2015, p. 43.

2 - La montée des discriminations

188. **La bande passante comme ressource rare** - Si les propriétaires d'infrastructures de télécommunications ont l'entière maîtrise physique de leurs matériels, l'âme de leurs réseaux est constituée par les protocoles. Or, nous avons vu qu'en application des principes du *end-to-end*, ceux qu'on appelle TCP/IP transforment leurs routeurs sophistiqués et leurs coûteuses fibres optiques en *dumb pipes*. Cela ne les empêche pas de percevoir un retour sur investissements : en tant que FAI, ils sont rémunérés par leurs propres abonnés, mais aussi par leurs concurrents avec lesquels ils passent des accords régissant l'interconnexion des réseaux³³. Et après tout, les services postaux transportent aveuglément les colis qui leur sont confiés. Pourquoi n'en irait-il pas de même avec le transport d'information ? Le problème est que le réseau serait menacé de congestion : si le volume d'information qu'il est possible d'y faire transiter pour une durée donnée a explosé depuis les années 80, les besoins ont augmenté plus vite encore. Il est tentant, dès lors, de définir des usages d'Internet qui peuvent attendre — les emails, par exemple — tandis que d'autres seraient traités en priorité — ainsi des flux vidéo. Cela revient à abandonner le principe des « meilleurs efforts » dans l'acheminement, en instaurant une hiérarchie entre contenus : certains paquets, pourtant premiers arrivés, ne seraient pas les premiers servis. Des solutions techniques sont alors développées pour rendre possible cette discrimination, regroupées sous l'appellation rassurante de « *Quality of service* » (QoS)³⁴. En pratique, divers indices seraient recherchés par les routeurs, qui leur permettraient de décider à quelle vitesse ils traitent les paquets qui leur sont adressés³⁵. D'abord, les logiciels communiquent en utilisant différents canaux numérotés, appelés ports, qui n'ont pas tous la même fonction : par exemple, un serveur de courrier sortant utilise généralement le port 25. L'analyse de ce paramètre permet donc parfois de déduire le type de contenu véhiculé. Il est ensuite possible de recourir aux plages d'adresses IP. Ainsi, les serveurs de YouTube ou de Dailymotion utilisent un ensemble de numéros contigus, qui constituent l'adresse à laquelle ils peuvent être contactés sur le réseau. Un routeur pourrait recevoir l'instruction d'accélérer ou de ralentir les paquets dont il est demandé la « livraison » à ces adresses. Il est encore envisageable d'utiliser certains champs, à l'heure actuelle rarement exploités, au sein de l'*Internet Protocol*, comme « *traffic class* », afin d'étiqueter volontairement des paquets d'information, qui seront reconnus par le réseau de communication et pourront être favorisés par lui. Enfin, lorsqu'aucune des méthodes simples citées précédemment n'est efficace, il reste possible de procéder à une analyse approfondie

33. - L. Chapin et C. Owens, « Interconnection and peering among internet service providers. A historical perspective. An interisle white paper », 2005, article consultable sur *interisle.net*, spéc. p. 19.

34. - L. Lessig, *L'avenir des idées*, op. cit., première partie, chapitre 2.

35. - A. Chaigneau, « Propriété et souveraineté de l'Internet... », art. préc., p. 21.

des paquets : le routeur ne se contentera pas de lire l'en-tête — qu'on peut assimiler à l'adresse sur une enveloppe — mais inspectera le contenu, à la lumière d'analyses statistiques antérieures, pour comprendre quel type d'informations il est en train de véhiculer³⁶.

189. Une grande variété d'atteintes - Ainsi les « tuyaux idiots » peuvent-ils se muer en canaux intelligents. Ces instruments techniques ont rendu possibles diverses atteintes à la neutralité du net, qui n'ont pas toutes la même intensité et ne poursuivent pas toutes la même finalité.

En 2007, le câblo-opérateur américain Comcast a bloqué la possibilité pour ses abonnés d'échanger des fichiers sur certains réseaux de pair-à-pair. La règle ainsi adoptée n'avait pas été dévoilée publiquement. Elle fut révélée par une série de tests réalisés à l'échelle nationale par l'agence *The Associated Press*³⁷. Ces mesures auraient ensuite été présentées comme permettant de lutter contre la congestion du réseau - sans que l'affirmation soit démontrée³⁸.

Plus récemment, le géant Verizon a été accusé de bloquer l'utilisation de l'application de paiement *Google Wallet* par les utilisateurs de son réseau. Le professeur de droit américain Barbara van Schewick avait déclaré qu'il s'agissait d'une violation de la neutralité du net, visant à défavoriser un concurrent :

*Verizon's behavior looks like an attempt to stall a competing mobile payment application until Verizon's own application is launched," van Schewick said in an email. "Verizon's behavior ... threatens competition and innovation in the emerging market for mobile payments. If Sprint, the nation's third largest wireless carrier, remains the only carrier that supports Google Wallet, Google Wallet will be dead upon arrival"*³⁹.

En France, des blocages ont également eu lieu : les opérateurs mobiles ont par exemple empêché, par le passé, l'usage d'applications de téléphonie par Internet (dites « de voix sur IP » ou « VoIP »), provoquant les foudres de la Commission européenne⁴⁰. Inversement, certains usages du réseau ont été favorisés : des forfaits étaient vendus sans accès à Internet, avec une exception en faveur des seuls Facebook et Twitter - ce qui peut s'analyser en un blocage du reste du réseau⁴¹.

36. - N. Anderson, « Deep packet inspection meets 'Net neutrality, CALEA », article *arsetechnica.com* du 26 juillet 2007.

37. - P. Svensson, « Comcast blocks some internet traffic », article *The Associated Press*, 19 octobre 2007.

38. - A. Chaigneau, « Propriété et souveraineté de l'Internet... », art. préc., p. 21.

39. - G. Gross, « Stanford professor files net neutrality complaint against Verizon Wireless », article *computerworld.com* du 19 décembre 2011.

40. - G. Champeau, « Bruxelles veut interdire le blocage de la VoIP sur les mobiles », article *numerama.com* du 7 décembre 2009.

41. - G. Champeau, « Sosh lance un forfait avec Facebook et Twitter illimités, sans Internet », article *numerama.com* du 6 février 2012. V. aussi infra, n°195.

Les atteintes à la neutralité du net ne se matérialisent pas nécessairement par des blocages purs et simples de services : il peut s'agir de ralentir certains flux au profit d'autres. Free avait été soupçonné par l'Autorité de Régulation des Communications Électroniques et des Postes (ARCEP) de ralentir volontairement la liaison de ses abonnés avec le site de vidéos YouTube, suite à des désaccords entre cet opérateur et Google sur la répartition des frais d'acheminement des informations. L'enquête s'est toutefois révélée infructueuse⁴². En revanche, Bouygues Telecom propose toujours à ses clients mobiles professionnels un service dit « internet prioritaire » : « en cas d'affluence sur le réseau 3G/4G, le débit reste plus rapide que celui des utilisateurs n'ayant pas le service Internet prioritaire sauf si le débit est réduit en raison d'échange de données très élevé »⁴³. Le réseau de communications ne se contente donc plus de faire ses « meilleurs efforts » en suivant le principe « premier arrivé, premier servi », mais donne la priorité aux paquets issus d'une clientèle plus lucrative ou jugée plus importante.

190. La diversité des réglementations concevables - Dans un article visionnaire datant de 2003, le juriste américain Tim Wu mettait en garde :

*Communications regulators over the next decade will spend increasing time on conflicts between the private interests of broadband providers and the public's interest in a competitive innovation environment centered on the Internet*⁴⁴.

Dans tous les exemples cités ci-dessus, ce ne sont pas les mêmes valeurs qui sont heurtées, ce ne sont pas les mêmes dangers qui se profilent. Il n'est donc pas surprenant que Madame Barbara van Schewick décèle, au sein des propositions de réglementation se proposant de « protéger la neutralité du net », des règles très différentes dans leur ambition comme dans leur contenu⁴⁵. Toutes ont en commun, dit-elle, d'interdire les blocages purs et simples de services⁴⁶. Nombre d'entre elles envisagent en revanche qu'une priorité puisse être consentie à certains flux d'informations : la

42. - Décision n° 2013-0987 de l'ARCEP en date du 16 juillet 2013 clôturant l'enquête administrative ouverte en application de l'article L. 32-4 du code des postes et des communications électroniques, relative aux conditions techniques et financières de l'acheminement du trafic entre diverses sociétés : « La congestion constatée aux heures de pointe affecte l'ensemble du trafic Internet acheminé en transit depuis et vers le réseau de Free, sans distinction de nature, d'origine ou de destination. Elle ne remet pas en cause la règle générale de partage équitable des ressources de capacité et de connectivité du réseau de l'opérateur entre les flux résultant du service d'accès à l'Internet, acheminés à travers les liens de transit. Le dimensionnement par Free de ces liens n'apparaît pas discriminatoire à l'égard de Google ou d'un autre FSCPL, ou d'une catégorie de service ou de contenu ».

43. - <https://www.bouyguestelecom.fr/forfait-professionnel-internet-mobile>.

44. - T. Wu, « Network neutrality, broadband discrimination », *Journal of Telecommunications and High Technology Law*, Vol. 2, p. 141, 2003, consultable en ligne sur ssrn.com.

45. - B. van Schewick, *Network neutrality and quality of service. What a non-discrimination rule should look like*, The Center for Internet and Society, 11 juin 2012 : <https://cyberlaw.stanford.edu/downloads/20120611-NetworkNeutrality.pdf>.

46. - *Ibid*, p. iv.

question est alors celle des critères retenus. Certaines réglementations peuvent viser exclusivement à sanctionner les atteintes à la concurrence : au cas par cas et *a posteriori* seraient punis les propriétaires de réseau ayant ralenti les flux en provenance de services concurrents des leurs⁴⁷. D'autres préfèrent poser des critères *a priori*, mais très permissifs : une atteinte à la neutralité du net serait permise chaque fois qu'elle fait l'objet d'une révélation explicite par l'opérateur : un tel système fait implicitement le pari que la concurrence sur le secteur est forte, que les consommateurs sont lucides — deux choses dont doute Madame van Shewick -, et laisse le marché décider⁴⁸. D'autres encore posent des critères *a priori*, mais plus sévères : il serait interdit de traiter différemment des usages similaires du net, relevant d'une même catégorie - *discrimination among like applications*⁴⁹. Ainsi deux sites de vidéo devraient-ils être traités de manière identique, de même que deux sites d'information, mais les flux vidéo pourraient par exemple bénéficier d'une priorité générale sur les flux correspondant à de l'information écrite. Le but serait d'assurer un grand confort dans la consommation des vidéos, contenus gourmands en bande passante, en pénalisant légèrement un autre média qui s'accommode mieux d'une réactivité plus faible. L'auteur considère toutefois cette approche comme dangereuse, en ce qu'elle permettrait des distorsions volontaires ou involontaires de concurrence, risquerait de brider l'innovation en se fondant sur l'état actuel de la technique, et reposerait sur une notion trop molle « d'usages similaires ».

Pour autant, Madame van Schewick n'est pas hostile aux discriminations, à condition qu'elles soient totalement neutres par rapport au type d'usage qui est fait de la bande passante - *application-agnostic*⁵⁰. Cela laisse subsister par exemple la possibilité de proposer des offres à débits différents et prix différents, des offres avec ralentissement au-delà d'un certain quota de données utilisé, voire une priorité générale des usagers payant plus cher.

*Application-agnostic network management coupled with user-controlled prioritization gives network providers the tools they need to maintain the quality of the Internet experience for all users, even during times of congestion, while preserving the application-blindness of the network and the principle of user choice to the extent possible. Network providers would be able to prevent aggressive users from overwhelming the network and enforce fairness among users by allocating bandwidth among users in application-agnostic ways. But how users use the bandwidth available to them, and whether they would like to give some of their applications priority over others, would be choices left to the users*⁵¹.

47. - *Ibid.*, p. viii.

48. - *Ibid.*, p. ix.

49. - *Ibid.*, p. xii.

50. - *Ibid.*, p. x.

51. - *Ibid.*, p. xi.

Ce dispositif serait complété par une clause de sauvegarde, permettant une discrimination entre les contenus dans les situations exceptionnelles de danger pour le réseau⁵².

Techniquement, cela revient certes à admettre que le réseau ne fait pas simplement ses « meilleurs efforts » pour acheminer systématiquement l'information d'un abonné, mais qu'il peut tenir compte du contexte - présence en ligne d'abonnés à une formule prioritaire, ou consommation par l'abonné de son quota mensuel d'Internet rapide. Mais la proposition semble bien équilibrée, et correspond même, peut-être, à l'idée intuitive que certains se font de la « neutralité » du net, puisqu'ici les ralentissements imposés aux utilisateurs sont totalement décorrélés de la nature des usages.

Parmi l'ensemble de ces possibilités, il est temps de révéler les choix qui ont été ceux de la France, de l'Europe, mais aussi des USA - dont les FAI possèdent une fraction considérable des infrastructures mondiales de télécommunication.

B - La réaction publique : imposer la neutralité du réseau

191. **Plan** - Jusqu'à une date très récente, l'histoire était celle d'une montée progressive de la neutralité du net dans les législations et décisions administratives. C'est encore ainsi que la situation européenne peut être présentée (1). Aux USA, en revanche, si le principe a été consacré en 2015, l'élection du président Donald Trump a marqué le début d'un net revirement sur cette question (2)⁵³.

1. - La faveur européenne

192. **La première position de l'Union : une simple exigence de transparence** - En 2009, l'Union européenne décide de mettre à jour un ensemble de textes relatifs aux communications électroniques, dont une directive de 2002 *concernant le service universel et les droits des utilisateurs au regard des réseaux et services de communications électroniques*⁵⁴. La question de la

52. - *Ibid.* : « *At the same time, the reasonable network-management exception provides a safety valve that allows network providers to react in more application-specific ways if a problem cannot be solved through application-agnostic means* ».

53. - Sur l'ensemble de ces questions : J. Cattat, « La protection de la neutralité de l'internet : pour un accès neutre aux biens numériques », art. préc. ; J. Cattat, *Le droit de l'accès aux communications électroniques*, préf. R. Mehdi et H. Isar, PUAM, 2015. *Adde* les rapports officiels cités dans les notes à suivre.

54. - Directive 2009/136/CE du Parlement européen et du Conseil du 25 novembre 2009 modifiant la directive 2002/22/CE concernant le service universel et les droits des utilisateurs au regard des réseaux et services de communications électroniques, la directive 2002/58/CE concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques et le règlement (CE) n° 2006/2004 relatif à la coopération entre les autorités nationales chargées de veiller à l'application de la législation en matière de protection des consommateurs.

neutralité du net surgit au cours des débats. La position adoptée par le législateur européen est alors teintée de prudence, si ce n'est de défiance. Il est notamment affirmé :

La présente directive ne prescrit ni n'interdit les conditions imposées par les fournisseurs de services et communications électroniques accessibles au public pour limiter l'accès des utilisateurs finals aux services et applications et/ou leur utilisation, lorsqu'elles sont autorisées par le droit national et conformes au droit communautaire, mais prévoit une obligation de fournir des informations concernant ces conditions⁵⁵.

Rappelons que selon Madame van Schewick, s'en remettre à une transparence de l'offre n'est raisonnable qu'à deux conditions. La première est que la concurrence soit suffisamment forte pour que des alternatives disposent d'alternatives pour le cas où la proposition ainsi formulée ne les satisferait pas. De ce point de vue, la situation française est peut-être meilleure que celle qui prévaut sur le marché américain. La seconde condition, c'est que les clients des FAI soient suffisamment compétents et avisés pour repérer l'existence de ces informations, les comprendre, et arbitrer en conséquence. Au moins s'agissant des simples consommateurs, et au regard de l'extrême technicité du sujet, il est permis d'en douter. Toutefois, si la directive n'imposait pas aux États d'aller plus loin, elle ne leur interdisait pas de le faire.

193. Les réactions françaises - La modification, par l'Europe, de ses grands textes relatifs aux communications électroniques, a rendu nécessaires plusieurs actes de transposition. En 2011, ceux-ci ont été l'occasion d'inscrire dans le Code des postes et des communications électroniques des dispositions allant dans le sens d'une neutralité des réseaux, par exemple :

II. – Dans le cadre de leurs attributions respectives, le ministre chargé des communications électroniques et l'Autorité de régulation des communications électroniques et des postes prennent, dans des conditions objectives et transparentes, des mesures raisonnables et proportionnées aux objectifs poursuivis et veillent :[...]

4° bis A l'absence de discrimination, dans des circonstances analogues, dans les relations entre opérateurs et fournisseurs de services de communications au public en ligne pour l'acheminement du trafic et l'accès à ces services [...]

15° A favoriser la capacité des utilisateurs finals à accéder à l'information et à en diffuser ainsi qu'à accéder aux applications et services de leur choix [...]⁵⁶.

Les pouvoirs de l'ARCEP ont ainsi été renforcés. Mais cela revenait à aborder la question de manière indirecte, quand il aurait été préférable de fixer nettement et sans détour les grands principes gouvernant la matière. Telle était la position d'un rapport parlementaire remis la même

55. - Art. 1.

56. - Art. L. 32-1 CPCE dans sa rédaction issue de l'ordonnance n° 2011-1012 du 24 août 2011 relative aux communications électroniques.

année par Mesdames Erhel et de La Raudière, et consacré à « la neutralité de l'Internet et des réseaux ». Il était notamment proposé de définir ainsi le principe de neutralité :

le principe de neutralité devrait être défini dans la loi comme :

(i) la capacité pour les utilisateurs d'Internet

(ii) d'envoyer et de recevoir le contenu de leur choix, d'utiliser les services ou de faire fonctionner les applications de leur choix, de connecter le matériel et d'utiliser les programmes de leur choix, dès lors qu'ils ne nuisent pas au réseau,

(iii) avec une qualité de service transparente, suffisante et non discriminatoire,

(iv) et sous réserve des obligations prononcées à l'issue d'une procédure judiciaire et des mesures nécessitées par des raisons de sécurité et par des situations de congestion non prévisibles⁵⁷.

Il s'agissait donc d'une prise de position forte en faveur d'une neutralité qui, pour reprendre la classification de Madame van Schewick, aurait été de type *application-agnostic*. La proposition n'a pas connu de traduction législative immédiate, mais elle a été reprise par plusieurs études ultérieures. Un rapport rendu par l'ARCEP en 2012 éclairait le Parlement et le Gouvernement sur les enjeux, tout en les laissant prudemment décider des suites à donner⁵⁸. En 2013, le Conseil National du numérique, au contraire, appelait vivement à la consécration législative « la plus large » possible⁵⁹. Quant au Conseil d'État, en 2014, il faisait d'une consécration de la neutralité des réseaux la deuxième proposition de son rapport consacré au numérique et aux droits fondamentaux⁶⁰.

Dans l'intervalle, la position des institutions européennes sur cette question avait largement évolué.

194. La consécration européenne - À l'issue de la révision des textes européens relatifs à la communication en 2009, la Commission européenne avait ouvert un cycle de réflexion sur la neutralité des réseaux⁶¹. En 2011, le Parlement avait adopté une résolution qui reconnaissait certes

57. - C. Erhel et L. de La Raudière, *Rapport d'information sur la neutralité de l'Internet et des réseaux*, enregistré à la Présidence de l'Assemblée nationale le 13 avril 2011.

58. - ARCEP, *Rapport au Parlement et au Gouvernement sur la neutralité de l'Internet*, sept. 2012.

59. - CNNum, *Rapport relatif à l'avis net neutralité n° 2013-1 du 1er mars 2013*. Le lecteur se reportera aux annexes de ce rapport pour un exposé détaillé des débats sur la neutralité du net en France, dans différents pays d'Europe et aux USA.

60. - Conseil d'État, *Le numérique et les droits fondamentaux*, rapport préc., p. 337. Les développements fondant cette proposition se trouvent p. 93 et s.

61. - V. not. la déclaration publiée au JO L 337 du 18 décembre 2009 et la communication au Parlement européen, au Conseil, au Comité économique et social européen et au Comité des régions du 19 avril 2011 sur l'Internet ouvert et la neutralité d'Internet en Europe.

« [...] la nécessité d'une gestion raisonnable du trafic afin de garantir que la connectivité des utilisateurs finaux n'est pas interrompue par une congestion du réseau [...] », mais qui

*[...] pri[ait] instamment les autorités nationales compétentes de s'assurer que les interventions sur la gestion du trafic n'impliquent pas de discrimination anticoncurrentielle; estime que la spécialisation (ou la gestion) des services ne devrait pas porter atteinte au maintien d'un accès à Internet solide, sans garantie de performances, favorisant ainsi l'innovation et la liberté d'expression, garantissant la concurrence et évitant une nouvelle fracture numérique [...]*⁶².

C'est dans ce contexte qu'a été élaboré, puis adopté en 2015, un règlement sur « l'internet ouvert »⁶³. Celui-ci proclame solennellement :

1. Les utilisateurs finals ont le droit d'accéder aux informations et aux contenus et de les diffuser, d'utiliser et de fournir des applications et des services et d'utiliser les équipements terminaux de leur choix, quel que soit le lieu où se trouve l'utilisateur final ou le fournisseur, et quels que soient le lieu, l'origine ou la destination de l'information, du contenu, de l'application ou du service, par l'intermédiaire de leur service d'accès à l'internet [...].

2. Les accords entre les fournisseurs de services d'accès à l'internet et les utilisateurs finals sur les conditions commerciales et techniques et les caractéristiques des services d'accès à l'internet, telles que les prix, les volumes de données ou le débit, et toutes pratiques commerciales mises en œuvre par les fournisseurs de services d'accès à l'internet, ne limitent pas l'exercice par les utilisateurs finals des droits énoncés au paragraphe 1.

*3. Dans le cadre de la fourniture de services d'accès à l'internet, les fournisseurs de services d'accès à l'internet traitent tout le trafic de façon égale et sans discrimination, restriction ou interférence, quels que soient l'expéditeur et le destinataire, les contenus consultés ou diffusés, les applications ou les services utilisés ou fournis ou les équipements terminaux utilisés*⁶⁴.

Le texte prévoit ensuite quelles mesures peuvent être prises lorsque des tensions apparaissent sur le réseau. Là réside sans doute le cœur du dispositif : admettre de trop larges dérogations aux principes qui viennent d'être énoncés les videraient de toute substance. C'est précisément dans les situations où la bande passante se fait rare que surgissent les tentations que le principe de neutralité du réseau a vocation à repousser. Le règlement est rassurant sur ce point. Il envisage d'abord les « mesures raisonnables de gestion du trafic » au quotidien : elles ne doivent pas discriminer selon

62. - Parlement européen, *Résolution sur l'Internet ouvert et la neutralité d'Internet en Europe*, 17 novembre 2011.

63. - Règlement (UE) 2015/2120 du Parlement européen et du Conseil du 25 novembre 2015 établissant des mesures relatives à l'accès à un Internet ouvert et modifiant la directive 2002/22/CE concernant le service universel et les droits des utilisateurs au regard des réseaux et services de communications électroniques et le règlement (UE) no 531/2012 concernant l'itinérance sur les réseaux publics de communications mobiles à l'intérieur de l'Union.

64. - Art. 3 du règlement 2015/2120 précité.

les contenus⁶⁵. Il prévoit ensuite des mesures de gestion pour les crises les plus graves, qui peuvent entraîner une discrimination selon les contenus, lorsque l'intégrité même du réseau est menacée ou lorsqu'une congestion exceptionnelle se profile⁶⁶. Cette combinaison d'un principe strict de non-discrimination et d'exceptions très étroitement encadrées correspond largement au modèle qui était préconisé par Madame van Schewick⁶⁷.

195. **L'accompagnement en droit français** - S'agissant d'un règlement européen, aucune mesure de transposition n'était à proprement parler nécessaire en droit français. Mais la loi République numérique a modifié une nouvelle fois le Code des postes et des communications électroniques, afin d'enrichir les pouvoirs de l'ARCEP, afin que l'autorité soit en mesure de contrôler au mieux les pratiques des acteurs de terrain⁶⁸. De plus, l'Organe des régulateurs européens des communications électroniques (ORECE) a publié un ensemble de lignes directrices pour guider les régulateurs nationaux dans l'application du règlement⁶⁹.

L'ARCEP a dressé un premier bilan de ses travaux en la matière dans un rapport publié en mai 2017⁷⁰. L'autorité y rappelle notamment qu'un certain nombre de blocages et d'interdictions avaient cours dans les offres des opérateurs français : interdiction du *peer-to-peer*, des *newsgroups*, du *streaming* vidéo, de l'utilisation d'un téléphone mobile comme relais pour accéder à Internet depuis un autre appareil. Ces pratiques seraient en voie de disparition⁷¹. En revanche, la pratique dite du *zero-rating* n'a pas disparu : il s'agit de proposer un forfait limité à une certaine quantité de données, mais de « compter comme zéro » la consommation dirigée vers un ou plusieurs services préalablement déterminés, comme Facebook. L'ARCEP rappelle, « sous réserve d'une analyse au cas par cas », qu'il s'agit probablement d'une pratique illégale⁷². À l'avenir, l'Autorité poursuivra ses campagnes de mesure de la qualité du service sur l'ensemble du territoire, mais annonce son intention de recourir au *crowdsourcing* — aux connaissances du public — pour compléter ses

65. - *Ibid.* : « Le premier alinéa n'empêche pas les fournisseurs de services d'accès à l'internet de mettre en œuvre des mesures raisonnables de gestion du trafic. Pour être réputées raisonnables, les mesures sont transparentes, non discriminatoires et proportionnées, et elles ne sont pas fondées sur des considérations commerciales, mais sur des différences objectives entre les exigences techniques en matière de qualité de service de certaines catégories spécifiques de trafic. Ces mesures ne concernent pas la surveillance du contenu particulier et ne sont pas maintenues plus longtemps que nécessaire ».

66. - *Ibid.*

67. - V. *supra*, n°190.

68. - Articles 40 et s. de la loi précitée n° 2016-1321.

69. - ORECE (BEREC selon l'acronyme anglais), *Guidelines on the Implementation by National Regulators of European Net Neutrality Rules*, 30 août 2016, consultables sur berec.europa.eu.

70. - ARCEP, *L'état d'Internet en France édition 2017*, mai 2017, consultable sur arcep.fr.

71. - *Ibid.*, p. 17.

72. - *Ibid.*

moyens. Un outil sera mis à la disposition de tous « pour mesurer la qualité de service et détecter les pratiques de gestion de trafic »⁷³. Il sera complété par un espace de signalement en ligne, permettant aux utilisateurs d’attirer l’attention du régulateur sur une pratique qui leur semble contraire au règlement européen⁷⁴. L’ARCEP entend également renforcer sa coopération avec d’autres services de l’État, comme la DGCCRF, mais aussi avec les autres régulateurs nationaux⁷⁵.

L’Europe a donc pris nettement position en faveur de la neutralité du net, entendue comme une neutralité des réseaux de transport de l’information. Elle en retient une conception à la fois exigeante et techniquement réaliste. Voyons à présent quelle est la position nord-américaine sur ces questions.

2 - Le revirement américain

196. La FCC à la recherche d’un fondement pour agir - Une grande partie de l’épine dorsale d’Internet est la propriété des FAI des États-Unis d’Amérique. Les décisions prises outre-Atlantique sont donc susceptibles d’avoir un impact sur le trafic mondial⁷⁶. S’il n’est pas utile, dans le cadre de cette étude, d’aller trop loin dans les spécificités du droit américain, il est donc nécessaire d’en peindre l’évolution à grands traits.

Comme l’écrit M. Jean Cattan, « L’histoire du débat sur la protection de la neutralité de l’internet aux États-Unis se résume en somme à la question de savoir sur laquelle [de] trois bases juridiques la [Federal Communications Commission] est fondée à agir »⁷⁷.

La première base juridique sur laquelle l’Autorité a tenté d’agir était le premier titre du *Communications Act* de 1934, relatif à ses pouvoirs généraux⁷⁸. Dès 2005, elle rendit sur ce fondement un *policy statement* adoptant les principes suivants :

To encourage broadband deployment and preserve and promote the open and interconnected nature of the public Internet, consumers are entitled to access the lawful Internet content of their choice.

To encourage broadband deployment and preserve and promote the open and interconnected nature of the public Internet, consumers are entitled to run applications

73. - *Ibid.*

74. - *Ibid.*

75. - *Ibid.*, p. 18.

76. - V. *supra*, n° 184.

77. - J. Cattan, « La protection de la neutralité de l’Internet... », art. préc., p. 45.

78. - Paragraphe 154, sous-chapitre 1, point (i) : « “*The Commission may perform any and all acts, make such rules and regulations, and issue such orders, not inconsistent with this chapter, as may be necessary in the execution of its functions*”.

and use services of their choice, subject to the needs of law enforcement.

To encourage broadband deployment and preserve and promote the open and interconnected nature of the public Internet, consumers are entitled to connect their choice of legal devices that do not harm the network

*To encourage broadband deployment and preserve and promote the open and interconnected nature of the public Internet, consumers are entitled to competition among network providers, application and service providers, and content providers*⁷⁹.

La FCC avait ainsi fait très tôt la démonstration de sa détermination à promouvoir la neutralité des réseaux. Toutefois, lorsqu'elle tenta de mettre en œuvre ces principes dans une affaire Comcast — dont le contexte a déjà été décrit⁸⁰ -, la Cour d'appel du district de Columbia refusa à l'Autorité le pouvoir de prendre de telles mesures sur le fondement de la section 1 du Communications Act, dans une décision rendue en 2010⁸¹.

Peu de temps après, la FCC essaya alors de recourir à une deuxième base juridique, issue du *Telecommunications Act* de 1996⁸². Le texte visé avait pour objectif de fournir un accès au réseau à l'ensemble de la population américaine. Il fallait donc solliciter quelque peu le texte pour y découvrir des principes relatifs à la neutralité du réseau. Cela n'empêcha pas la FCC d'adopter un *Open internet order*, qui fut rapidement contesté par l'opérateur Verizon⁸³. À nouveau, la Cour d'appel du district de Columbia fit s'écrouler l'édifice, par un arrêt de janvier 2014⁸⁴.

197. La consécration de 2015 - Quelques mois plus tard, le président Obama encouragea à prendre de nouvelles mesures, en suggérant d'employer une troisième base légale, le titre 2 du *Communications Act*, consacré aux *common carriers*⁸⁵. Le 12 mars 2015, la FCC adopta un nouvel *Open Internet rules*⁸⁶. Celui-ci comportait trois « *bright line rules* » :

79. - *FCC policy statement*, 05-151, 5 août 2005, consultable sur apps.fcc.gov.

80. - V. *supra*, n° 189.

81. - Court of Appeal for the district of Columbia circuit, 6 avril 2010, n° 08-1291, *Comcast corporation V. Federal communications Commission and United States of America*.

82. - La section 706 dispose : « *The Commission and each State commission with regulatory jurisdiction over telecommunications services shall encourage the deployment on a reasonable and timely basis of advanced telecommunications capability to all Americans (including, in particular, elementary and secondary schools and classrooms) by utilizing, in a manner consistent with the public interest, convenience, and necessity, price cap regulation, regulatory forbearance, measures that promote competition in the local telecommunications market, or other regulating methods that remove barriers to infrastructure investment* ».

83. - FCC, *Report and Order. Preserving the Open Internet Broadband Industry Practices*, 10-201, 21 décembre 2010.

84. - Court of Appeal for the district of Columbia circuit, 14 janvier 2014, n° 11-1355, *Verizon v. Federal Communications Commission*.

85. - E. Mechaber, « President Obama urges FCC to implement stronger net neutrality rules », article du 10 novembre 2014, obamawhitehouse.archives.gov.

86. - FCC, *Report and order on remand, declaratory ruling, and order*, 15-24, 12 mars 2015.

No Blocking: broadband providers may not block access to legal content, applications, services, or non-harmful devices.

No Throttling: broadband providers may not impair or degrade lawful Internet traffic on the basis of content, applications, services, or non-harmful devices.

No Paid Prioritization: broadband providers may not favor some lawful Internet traffic over other lawful traffic in exchange for consideration of any kind—in other words, no "fast lanes." This rule also bans ISPs from prioritizing content and services of their affiliates⁸⁷.

Une nouvelle fois saisie, la Cour d'appel du district de Columbia rendit cette fois-ci une décision favorable à la FCC, durant l'année 2016⁸⁸. M. Barack Obama salua la décision en termes chaleureux, et rendit hommage aux 4 millions d'Américains ayant assailli la FCC de messages en faveur de la neutralité du net, à l'occasion de la consultation publique qu'elle avait lancée⁸⁹.

L'arrivée à la Maison-Blanche de M. Donald Trump fit une nouvelle fois la démonstration de l'influence du Président sur la FCC, mais cette fois-ci en sens inverse.

198. Le coup d'arrêt de 2017 - En mars 2016, le commissaire de la FCC Ajit Pai avait diffusé une déclaration publique très hostile à l'*Open internet rules*. Il y accusait la présidence Obama d'avoir forcé la main de son institution, et critiquait vivement les règles adoptées sur le fond⁹⁰. C'est lui qui fut nommé à la tête de la Commission après l'élection du Président Trump, dans le but avoué de revenir sur la neutralité du réseau⁹¹. En mai 2017, un *notice of proposed rulemaking* baptisé

87. - Résumé des règles proposé par la FCC : <https://www.fcc.gov/general/open-internet>.

88. - Court of Appeal for the district of Columbia circuit, 14 juin 2016, n° 15-1063, *United States Telecom Association et al. v. Federal Communications Commission and United States for America*. Traduction proposée par J. Cattani, « La protection de la neutralité de l'Internet... », art. préc., p. 52 : « - Pas de blocage : les fournisseurs d'accès au haut débit ne peuvent pas bloquer l'accès au contenu, aux applications, aux services légaux ou aux terminaux non nuisibles. - Pas de ralentissement : les fournisseurs d'accès au haut débit ne peuvent pas altérer ou dégrader le trafic Internet légal selon le contenu, les applications, les services légaux ou aux terminaux non nuisibles en cause. - Pas de priorisation payante : les fournisseurs d'accès au haut débit ne peuvent pas favoriser un trafic Internet légal sur un autre trafic légal pour quelque considération que ce soit – en bref, pas de 'ligne rapide'. Les fournisseurs d'accès ne peuvent pas non plus prioriser leur contenu ou celui de leur société affiliée. »

89. - Une reproduction de la lettre ouverte peut être consultée à <https://obamawhitehouse.archives.gov/net-neutrality>. L'humoriste John Oliver a joué un rôle prépondérant dans le raz-de-marée de commentaires ayant déferlé sur la FCC. Au cours de son émission de télévision à succès, il avait vivement encouragé les spectateurs à intervenir. V. par ex. S. Nadia McDonald, « John Oliver's neut neutrality rant may have caused FCC site crash », article *washingtonpost.com* du 4 juin 2014.

90. - A. Pai, « Statement on the release of senate report on how the white house bowled over FCC independence », *FCC news*, 1er mars 2016 : « The report released yesterday by Chairman Ron Johnson of the Senate Committee on Homeland Security and Government Affairs paints a devastating portrait of the process that led to the adoption of President Obama's plan to regulate the Internet on February 26, 2015. It explains in painstaking detail how the FCC succumbed to White House pressure and forfeited its independence by agreeing to apply Depression-era rules to the Internet [...] » (https://apps.fcc.gov/edocs_public/attachmatch/DOC-337976A1.pdf).

91. - V. par ex. G. Pépin, « Trump nommé un ennemi de la neutralité du Net à la tête de la FCC », article

Restoring internet freedom fut publié et ouvert aux commentaires du public⁹². L'introduction du document était limpide :

Americans cherish a free and open Internet. And for almost twenty years, the Internet flourished under a light-touch regulatory approach [...]. But two years ago, the FCC changed course. It decided to apply utility-style regulation to the Internet. This decision represented a massive and unprecedented shift in favor of government control of the Internet. The Commission's Title II Order has put at risk online investment and innovation, threatening the very open Internet it purported to preserve. Investment in broadband networks declined. Internet service providers have pulled back on plans to deploy new and upgraded infrastructure and services to consumers. This is particularly true of the smallest Internet service providers that serve consumers in rural, low-income, and other underserved communities. Many good-paying jobs were lost as the result of these pull backs [...].

L'argument économique fut au centre des débats : en restreignant le pouvoir des propriétaires de réseaux de jouir de leur chose comme ils l'entendent et de fixer librement leur modèle économique, on réduirait les incitations à investir. En somme, en voulant imposer par la force de la loi un réseau souple et ouvert à l'innovation, on transformerait les infrastructures en champ de ruines déserté par les capitaux privés. À une FCC idéaliste succéderait une Commission lucide et pragmatique. Mais la bataille de chiffres fut rude : l'*Internet association* — qui regroupe l'essentiel des géants du numérique, mais certes pas les petits FAI auxquels la FCC fait référence — produisit un ensemble d'études montrant que les investissements dans les grands équipements de télécommunication ont continué à croître régulièrement depuis que se profile une application des principes de neutralité du réseau⁹³. Cela n'empêcha pas l'adoption du *Restoring internet freedom order* le 14 décembre 2017⁹⁴.

Par ailleurs, les mêmes pratiques de *zero rating* contre lesquelles l'ARCEP s'insurge actuellement en France faisaient l'objet d'enquêtes de la part de la FCC. La nouvelle direction de la Commission a décidé d'y mettre fin⁹⁵. Avant même les résultats de la consultation sur *Restoring internet freedom*, le cap est donc clairement fixé.

nextinpact.com du 24 janvier 2017.

92. - <https://www.fcc.gov/document/restoring-internet-freedom-notice-proposed-rulemaking>.

93. - Une large batterie d'indicateurs, avec leurs sources, peut être consultée sur : <http://netneutrality.internetassociation.org/facts/>. La liste des membres de l'Internet association est consultable à l'adresse <http://internetassociation.org/our-members/>.

94. - FCC, *Declaratory ruling, Restoring Internet Freedom, report and order*, FCC 17-166.

95. - G. Gebhart et E. Harmon », FCC abandons zero-rating investigation and moves backward on net neutrality », article *eff.org* du 9 février 2017. Sur l'attitude de l'ARCEP, V.supra, n°195.

II - La coordination

199. **Les standards communs** - La manière dont le réseau Internet global est conçu n'impose pas que la construction et le développement des infrastructures de communication fassent l'objet d'une planification mondiale précise. Il tolère fort bien le désordre : que des câbles ou des réseaux entiers soient ajoutés ou retranchés, et les routeurs s'adapteront. Si un chemin permettant la transmission d'informations entre les correspondants existe, il sera trouvé. Tant mieux s'il est court, tant pis s'il est long.

Le choix des standards techniques et protocoles à employer est une tout autre question. Pour que le golem de fibres et d'ondes se tienne, il faut un liant ; pour que les excroissances qui le constituent puissent dialoguer entre elles, une langue commune est nécessaire. Il n'est pas possible, ici, d'agir en ordre dispersé. Pour cette raison, une galaxie de groupes d'experts a été constituée au niveau mondial, dont les deux plus importants sont le *World Wide Web Consortium* (W3C) et l'*Internet Engineering Task Force* (IETF), ce dernier étant membre d'une association à objet plus vaste appelée Internet Society. Le W3C formule des propositions s'agissant des langages structurant les contenus sur Internet (notamment le HTML), tandis que l'IETF a en charge les protocoles de communication (notamment ceux qui constituent l'ensemble appelé TCP/IP)⁹⁶. Ces groupes d'ingénieurs, souvent présidés par des pionniers du net, réalisent un travail d'une grande technicité, mais dont l'analyse juridique est assez simple. Leurs propositions n'ont aucun caractère obligatoire. Simplement, dans la mesure où elles sont les meilleures et les plus convaincantes, et puisqu'il est nécessaire que tous les acteurs mondiaux choisissent une solution pour assurer le fonctionnement, ce qu'ils suggèrent est suivi d'effet. Le Conseil d'État y voit une victoire du droit souple, et ne manque pas de s'en féliciter⁹⁷.

La propriété, en l'occurrence la propriété intellectuelle, a joué un rôle prépondérant dans l'histoire de ces protocoles : un rôle négatif, celui d'un repoussoir. Tim Berners-Lee est l'un des inventeurs du HTML, le langage sur lequel repose cette partie d'Internet qu'on appelle le *World Wide Web*⁹⁸. Il raconte comment, dans les années 90, le protocole *Gopher* s'était largement imposé pour construire les sites Web, alors même qu'il imposait une architecture uniforme et très rigide, sous forme de menus, pour la présentation des informations. Le HTML, quoique supérieur, n'intéressait guère, jusqu'à ce que l'Université du Minnesota, propriétaire des droits sur le *Gopher*,

96. - Conseil d'État, *Le numérique et les droits fondamentaux*, rapport préc., p. 136. Adde les sites Internet de ces organisations : www.ietf.org et www.w3.org.

97. - *Ibid.*

98. - V. déjàsupra, n°11.

envisage de faire payer une contribution modique à chaque site utilisant son invention⁹⁹. Le CERN, employeur de Berners-Lee, mit au contraire les droits du protocole HTML dans le domaine public, ce qui assura son succès¹⁰⁰. Depuis lors, les grands protocoles sur lesquels repose Internet sont conçus par tous comme nécessairement libres de droits.

200. Les adresses IP et noms de domaine - Une autre question requiert une coordination de niveau mondial : celle des adresses Internet. Des luttes de pouvoir plus rudes s'y rencontrent qu'en matière de conception des protocoles. Une brève présentation technique permettra de comprendre pour quelles raisons. L'espace urbain est découpé en rues, dans lesquelles chaque immeuble se voit attribuer un numéro. Ces informations sont indispensables aux transporteurs de courriers et colis, qui les associent enfin à un nom pour trouver une boîte aux lettres. Un cube de métal de quelques dizaines de centimètres de côté est ainsi désigné, d'une manière unique dans le monde, par quelques lignes d'information. Sur Internet, les points d'où partent et arrivent les données se voient eux aussi assigner une adresse *Internet Protocol*, qui prend la forme d'une série de chiffres. Dans la version 4 du protocole IP, actuellement la plus répandue, 4 nombres compris entre 0 et 255 suffisent, chacun étant séparé par un point, par exemple : 192.168.0.1¹⁰¹.

De là naît une première difficulté : une même adresse IP ne doit pas être attribuée en deux points différents du réseau global. Quelqu'un ou quelque chose doit donc procéder à la distribution, en ayant une connaissance exhaustive de la situation mondiale.

De plus, la mémoire humaine est ainsi faite qu'il lui serait difficile de retenir de telles adresses sous forme numérique¹⁰². Le *Domain Name System* résout cette difficulté. Il peut être décrit comme un annuaire. De même qu'un annuaire téléphonique apparie une identité civile ou commerciale avec un numéro de téléphone, le DNS est capable de fournir une adresse IP à qui lui présente un nom de domaine - et inversement.

L'ensemble de ce système est aux mains d'une entité dénommée *Internet Corporation for Assigned Names and Numbers* ou ICANN¹⁰³. C'est elle qui assure le contrôle ultime des noms de

99. - Tim Berners-Lee, *Weaving the Web...*, op. cit., p. 40 et 72 s.

100. - L. Lessig, *L'avenir des idées*, op. cit., première partie, chapitre 2.

101. - Ce système fournit environ 4,3 milliards d'adresses distinctes, ce qui sera bientôt insuffisant, en raison notamment du développement des objets connectés. Il sera bientôt remplacé par la version 6 du protocole, qui offrira 3,4 fois 10 puissance 38 adresses différentes, ce qui représente « autant d'adresses que l'IP version 4 pour chaque étoile dans l'univers » (<http://www.worldipv6launch.org/infographic/>). À court terme, une adresse IP aura une apparence du type : 2001:db8:a0b:12f0::1.

102. - Ajoutons qu'un même service peut changer d'adresse IP au fil du temps.

103. - Pour une présentation générale de l'organisation et de ses missions : ICANN, *Guide d'initiation à*

domaine, ressources rivales — il n’y a qu’un seul « hotels.com » — dont la valeur économique peut être considérable. C’est d’elle que dépend, en dernier ressort, la capacité qu’ont les machines connectées au réseau à se retrouver les unes et les autres. Si ses structures se révélaient vulnérables aux attaques, des individus mal intentionnés pourraient rediriger massivement les internautes recherchant un nom de domaine vers des pages contrefaites. Le pouvoir de cette organisation est donc considérable, et il repose sur une infrastructure objet d’un droit de propriété. Les protocoles dont il était précédemment question sont des œuvres de l’esprit, mises en œuvre de manière décentralisée par l’ensemble des propriétaires de réseaux de communications ou par les créateurs de contenus en ligne. L’ICANN, en revanche, est propriétaire d’un matériel nécessaire au fonctionnement même du réseau. Après avoir rappelé dans quelles circonstances l’ICANN est apparue (A), la question de sa gouvernance sera posée (B).

A - La naissance de l’ICANN : une structure privée américaine au pouvoir mondial

201. **Le DNS et les « clés d’Internet »** - Quatre fois par an, une étrange « cérémonie des clés » se déroule dans des locaux contrôlés par l’ICANN. Quelques individus — le chiffre de sept est avancé — arrivent de partout dans le monde. Ensemble, ils se rendent au plus profond d’un bâtiment anonyme, dans une zone industrielle sans âme. Chacun d’entre eux se soumet à un scan de la rétine, saisit un code PIN sur un clavier, puis entre dans la salle où sera célébré l’office païen qui redonnera vigueur pour quelques mois à l’Internet mondial. Là, il sort la clé secrète dont il est porteur, et l’associe à ses semblables. En dépit de sa troublante ressemblance avec les scènes de fiction où le S.P.E.C.T.R.E complotte pour prendre le contrôle du monde libre, cette séquence n’a rien d’imaginaire. Elle est certes romancée par les médias, qui la trouvent fascinante¹⁰⁴. Le symbole est fort, quoi qu’il en soit : ce centre névralgique du réseau global qu’est le *Domain Name System* n’est pas une vue de l’esprit, mais prend la forme de couloirs surveillés par des caméras, de cartes magnétiques et surtout de puissants serveurs, objets d’un droit de propriété privée.

Dans les années 80, une personne ou organisation souhaitant connecter une nouvelle machine au réseau global issu d’ARPANET devait contacter par téléphone le *Network Information Center* du *Stanford Research Institute*. Madame Elizabeth Feinler décrochait, s’enquêrait des besoins de son

l’ICANN, disponible sur icann.org.

104. - V. par ex. cet article, accompagné d’une vidéo de la « cérémonie » : J. Ball, « Meet the seven people who hold the keys to the worldwide internet security », article *theguardian.com* du 28 février 2014. V. aussi le compte-rendu par de la première cérémonie : ICANN, « Major milestone for the internet and ICANN. The Key Signing ceremony is now complete », publication icann.org du 16 juin 2010.

interlocuteur, puis lui attribuait un nom et une adresse¹⁰⁵. « Le problème, c'est que le service était indisponible les week-ends et la semaine de Noël », relève malicieusement M. Paul Mockapetris, qui décida d'y remédier en inventant le DNS avec M. John Postel¹⁰⁶. Avant cela, l'ensemble des adresses disponibles sur ARPANET figuraient dans un unique fichier maîtrise appelé `hosts.txt`¹⁰⁷. M. Mockapetris a imaginé une architecture pyramidale, qui fonctionne comme suit. Le sommet de la pyramide est constitué d'un petit nombre de serveurs racines, dont le contenu est considéré comme parfaitement fiable. Les informations qu'ils contiennent sont ensuite disséminées vers les étages inférieurs, vers des serveurs DNS de plus en plus décentralisés. Lorsqu'un internaute tape un nom de domaine dans la barre d'adresse de son navigateur, ou clique sur un lien qui contient un tel nom de domaine, il se connecte généralement au serveur DNS de son FAI. Si celui-ci ignore à vers quelle adresse IP chiffrée il doit renvoyer, il s'adresse à des serveurs situés plus haut dans la chaîne, qui eux-mêmes pourront remonter aussi loin que nécessaire. Une fois que les serveurs des niveaux inférieurs ont répondu à la requête, ils la gardent en mémoire pendant un certain temps. Ceci leur évitera de solliciter systématiquement le sommet de la pyramide, qui n'aurait pas les capacités matérielles pour faire face à des requêtes trop nombreuses. Au bout d'un moment, toutefois, les serveurs décentralisés prendront soin de « rafraîchir » l'information dont ils disposent, ce qui autorise le titulaire d'un nom de domaine à changer l'adresse IP correspondante si cela est nécessaire. Ce changement sera rapidement enregistré dans les serveurs DNS des niveaux les plus élevés, et se diffusera vers le bas au fil des heures.

Pour qu'un tel système pyramidal fonctionne, il faut s'assurer que l'information n'a pas été falsifiée, et que l'identité des serveurs DNS de haut niveau n'a pas été usurpée par une entité hostile. Il a déjà été exposé qu'une des fonctions du chiffrement consiste précisément à s'assurer à la fois de l'identité d'un correspondant lors d'une communication en ligne, par l'intermédiaire de « signatures », et de l'intégrité des informations échangées¹⁰⁸. La confiance inspirée par les serveurs DNS racine se prolonge ainsi le long de la chaîne. La « cérémonie des clés » consiste en réalité à renouveler les signatures chiffrées employées, quatre fois par an, afin de réduire la probabilité que le secret soit percé par un attaquant disposant de moyens considérables : il n'aura pas le temps d'y parvenir que la réponse à trouver aura déjà été modifiée¹⁰⁹.

105. - C. Metz, « Before Google and Godaddy, there was Elizabeth Feinler », article *wired.com* du 18 juin 2012.

106. - C. Metz, « Why does the net still work on Christmas ? Paul Mockapetris », article *wired.com* du 23 juillet 2012 : « The problem is that SRI was off during Christmas week, and they went home on weekdays ».

107. - M. D. Kudlick, « Host names on-line », 10 janvier 1974 : <https://tools.ietf.org/html/rfc608>.

108. - V. supra, n° 40.

109. - ICANN, « Major milestone for the internet... », art préc. : « During the ceremony, participants were present within a secure facility and witnessed the preparations required to ensure that the so-called key-signing-

202. La distribution des IP et domaines - Le DNS est un système qui permet *d'informer* les machines du monde entier du *résultat* de l'attribution des IP et noms de domaine. Il ne préjuge pas de la manière dont cette allocation sera effectuée en amont. Ces deux missions distinctes ont d'abord été assumées par des personnes physiques, dont la plus célèbre est le susnommé Jon Postel¹¹⁰. De 1976 à 1998, il exerce pratiquement seul les fonctions de ce qui deviendra l'*Internet Assigned Numbers Authority* (IANA) au sein de son institution de rattachement, l'*University of Southern California*¹¹¹.

En 1998, il utilisa son autorité personnelle pour modifier la tête de la pyramide constituant le serveur DNS, la faisant brièvement échapper au contrôle du gouvernement américain, sous lequel elle se trouvait de fait avant sa manœuvre¹¹². Prenant sans doute conscience du pouvoir dont disposait cet homme seul, le Département du Commerce américain, poussé par la présidence Clinton, lança une consultation visant faire échapper l'IANA à l'omnipotence de son fondateur. La solution préconisée visait — au moins en apparence — à relâcher la tutelle gouvernementale au profit d'une structure privée multipartite à but non lucratif. Dans une note restée célèbre, la *National Telecommunications and informations administration* écrivait notamment :

*Certain technical management functions require coordination. In these cases, responsible, private-sector action is preferable to government control. A private coordinating process is likely to be more flexible than government and to move rapidly enough to meet the changing needs of the Internet and of Internet users. The private process should, as far as possible, reflect the bottom-up governance that has characterized development of the Internet to date*¹¹³.

key (KSK) was not only generated correctly, but that almost every aspect of the equipment, software and procedures associated with its generation were also verified to be correct and trustworthy. The ceremony was conducted with the goal of ensuring that there is widespread confidence throughout the technical Internet community that the root zone, once signed, can be relied upon to protect users from false information ».

110. - Sur le parcours de ce pionnier d'internet, et le rôle qu'il joua dans la conception de multiples inventions et protocoles fondamentaux, V. not. « A ten year tribute to Jon Postel » : <http://www.internetsociety.org/what-we-do/grants-and-awards/awards/postel-service-award/ten-year-tribute-jon-postel>.

111. - J. Snyder, K. Komaitis et A. Robachevsky, « The history of IANA : an extended timeline with citations and commentary », janvier 2017, p. 2. Article publié sur le site de l'Internet society : <http://www.internetsociety.org/ianatimeline>.

112. - Ibid. : « January 28, 1998 : Postel emails the operators of the non-US Government root servers and asks that they use a server at IANA (dnsroot.iana.org) for authoritative root zone information rather than the "A" root server (a.root-servers.net) at Network Solutions. This effectively moved control of the DNS root from Network Solutions and the US Government to IANA—and immediately created a firestorm of controversy. On Feb 3, Postel requested that the change be backed out and that root updates should be taken from the "A" root server. Postel explained the change as a technical experiment, but not everyone is satisfied with this explanation. The unexpected nature of the change and the ability for a single individual take control over the DNS acts as a wakeup call serves to accelerate the process that would eventually lead to the formation of ICANN ».

113. - National Telecommunications and information administration, United States Department of Commerce, « Improvement of technical management of Internet names and addresses. Proposed rule », 20 février 1998 : <https://www.ntia.doc.gov/federal-register-notice/1998/improvement-technical-management-internet-names-and->

La même année, une personne morale à but non lucratif de droit californien fut donc créée, qui fut baptisée *Internet Corporation for Assigned Names and Numbers* (ICANN). Un contrat fut signé avec le Département du commerce, lui permettant de reprendre à son compte les fonctions dévolues à l'IANA¹¹⁴. Avant d'abandonner toute forme de tutelle sur ces questions, le Département y affirmait tester la capacité du secteur privé à les prendre en charge, et se laissait la possibilité de mettre fin à l'expérience après quelques années, si elle se révélait infructueuse¹¹⁵. Les grands principes que l'ICANN s'engageait à suivre étaient les suivants :

1. *Stability : This Agreement promotes the stability of the Internet and allows the Parties to plan for a deliberate move from the existing structure to a private-sector structure without disruption to the functioning of the DNS. The Agreement calls for the design, development, and testing of a new management system that will not harm current functional operations.*
2. *Competition : This Agreement promotes the management of the DNS in a manner that will permit market mechanisms to support competition and consumer choice in the technical management of the DNS. This competition will lower costs, promote innovation, and enhance user choice and satisfaction.*
3. *Private, Bottom-Up Coordination : This Agreement is intended to result in the design, development, and testing of a private coordinating process that is flexible and able to move rapidly enough to meet the changing needs of the Internet and of Internet users. This Agreement is intended to foster the development of a private sector management system that, as far as possible, reflects a system of bottom-up management.*
4. *Representation : This Agreement promotes the technical management of the DNS in a manner that reflects the global and functional diversity of Internet users and their needs. This Agreement is intended to promote the design, development, and testing of mechanisms to solicit public input, both domestic and international, into a private-sector decision making process. These mechanisms will promote the flexibility needed to adapt to changes in the composition of the Internet user community and their needs¹¹⁶.*

C'est ainsi qu'une association sans but lucratif californienne s'est retrouvée dotée de l'incroyable pouvoir d'attribuer les IP et les domaines. À première vue, il s'agit de découper en tranches un royaume imaginaire et de distribuer des abstractions : des droits de présenter une machine sur le réseau global sous une certaine identité, formulée d'une part en chiffres, d'autre part en lettres.

addresses-proposed-.

114. - Memorandum of understanding between the US Department of Commerce and Internet Corporation for Assigned Names and Numbers, 25 novembre 1998, dont le texte est disponible ici : <https://www.icann.org/resources/unthemed-pages/icann-mou-1998-11-25-en>.

115. - *Ibid.* : « Before making a transition to private sector DNS management, the DOC requires assurances that the private sector has the capability and resources to assume the important responsibilities related to the technical management of the DNS ».

116. - *Ibid.*

Historiquement, ce contrôle par l'ICANN d'un centre névralgique du réseau est pourtant la suite d'une emprise bien tangible, correspondant à la propriété privée reconnue à des universités américaines sur les structures devenues le DNS. Ce pouvoir s'est sédimenté jusqu'à devenir irréversible. L'ICANN contrôle les IP ; l'ICANN contrôle le DNS. Mais qui contrôle à présent l'ICANN ?

B - L'évolution de l'ICANN : la gestion d'un commun par le consensus ?

203. **Le secteur privé en dessous de l'ICANN** - Les principes fondateurs de l'ICANN énoncés ci-dessus matérialisent la foi américaine dans la supériorité du secteur privé, lorsqu'il s'agit de distribuer ces ressources rares que sont les noms de domaine. L'association californienne n'agit pas par elle-même : elle délègue la gestion des *Top Level Domains* (TLD), ou noms de domaines de premier niveau, à d'autres entités appelées « registres de noms de domaine ». Par exemple, dans l'adresse u-picardie.fr, .FR est un TLD. Le .FR est ainsi géré par l'Association française pour le nommage Internet en coopération (AFNIC)¹¹⁷. L'AFNIC passe elle-même des contrats avec des « bureaux d'enregistrement », ou « registraires », qui sont quant à eux des acteurs privés à vocation lucrative¹¹⁸. Ils constituent un réseau de distribution des noms de domaine de second niveau — par exemple, « lemonde.fr » — au plus près du terrain, mettent en œuvre des stratégies commerciales et disposent de services d'accompagnement des consommateurs.

204. **Le secteur privé au-dessus de l'ICANN** - Faire confiance aux acteurs privés pour commercialiser les noms de domaine est une chose. Leur confier la direction de l'ICANN en est une autre, mais c'est bien le choix qui a été fait. La manière dont sont formulées les bylaws qui gouvernent l'association parle d'elle-même :

[...] ICANN commits to do the following [...] : (iv) Employ open, transparent and bottom-up, multistakeholder policy development processes that are led by the private sector (including business stakeholders, civil society, the technical community, academia, and end users), while duly taking into account the public policy advice of governments and public authorities¹¹⁹.

117. - Avant 1998, il était géré par l'INRIA : comme aux USA, un Centre de recherche public a donc laissé sa place à une association de droit privé : <https://www.afnic.fr/fr/l-afnic-en-bref/presentation/missions-de-l-afnic-et-axes-strategiques-2017-2019-6.html>.

118. - Pour la vente des domaines gérés par l'AFNIC, on en recense plus de 400 : <https://www.afnic.fr/fr/votre-nom-de-domaine/comment-choisir-et-creer-mon-nom-de-domaine/trouver-mon-bureau-d-enregistrement-8.html>.

119. - *Bylaws for Internet Corporation For Assigned Names And Numbers. A California Nonprofit Public-Benefit Corporation*, Section 1.2. commitments and core values, (a) commitments, (iv) : <https://www.icann.org/resources/pages/governance/bylaws-en>.

Même si le secteur privé dont il est ici question dépasse largement le secteur marchand, et englobe notamment la communauté des chercheurs et des experts, c'est bien lui qui est chargé de concevoir les politiques appliquées par l'association. Les autorités publiques, regroupées dans un *Governmental Advisory Committee*, sont cantonnées à un rôle consultatif¹²⁰. Le postulat est simple : une représentation suffisamment exhaustive des parties prenantes dans le fonctionnement de l'Internet global est organisée. Elle doit mener à une gouvernance par consensus, l'addition entre intérêts particuliers conduisant au respect de l'intérêt général¹²¹. Ici encore, il s'agirait de préserver Internet en tant qu'il constitue un bien commun d'intérêt mondial.

205. **À la recherche d'une légitimité** - À en croire le professeur américain Jonathan Weinberg, cette promesse d'une *multistakeholder policy* n'a pas suffi, lors de la création de l'ICANN, à assoir aussitôt sa légitimité auprès des principaux intéressés¹²². En confiant à cette association la gestion du DNS, le Gouvernement américain délégua un pouvoir dont il n'était jusque-là pas titulaire, puisqu'il appartenait en réalité à des universités¹²³. D'ailleurs, priée de signer un accord de transfert de l'IANA au bénéfice de l'ICANN, l'*University of Southern California* traîna des pieds, même si elle finit par obtempérer¹²⁴. Il fallut ensuite convaincre les opérateurs des registres nationaux de contracter avec l'ICANN. Celle-ci, en tant que propriétaire des ressources formant la racine du DNS, était théoriquement en position de force, mais M. Weinberg estime que le Gouvernement des USA n'aurait pas autorisé la suppression pure et simple des pays réticents dans le sommet de la pyramide : « *In a worstcase analysis, governments, Internet service providers, or major institutional users could establish a consortium of alternative root servers outside of ICANN's*

120. - Un peu plus loin, il est encore précisé : « *While remaining rooted in the private sector (including business stakeholders, civil society, the technical community, academia, and end users), recognizing that governments and public authorities are responsible for public policy and duly taking into account the public policy advice of governments and public authorities* » : même section, (b), (vi). Le Governmental Advisory Committee possède son propre site Internet, consultable à l'adresse gacweb.icann.org.

121. - *Ibid.*, (vii) : « *Striving to achieve a reasonable balance between the interests of different stakeholders, while also avoiding capture [...]* ».

122. - J. Weinberg, « ICANN and the problem of legitimacy », *Duke law journal*, vol. 50:187, p. 187.

123. - *Ibid.*, p. 213 : « *The U.S. government, after all, had never managed the DNS through command-and-control regulation, and it had no command-and-control authority to delegate.137 ICANN was in a position to control other DNS actors only by entering into contracts in which those actors agreed to be bound* ».

124. - *Ibid.*, p. 214 : « *NSI was reluctant to recognize ICANN (which it correctly saw as a threat to its autonomy), but the Department of Commerce138 was in a position to assist ICANN with that relationship* ». L'accord suivant fut signé : USC/ICANN transition agreement, décembre 1999 (<https://www.icann.org/resources/unthemed-pages/usc-icann-transition-2012-02-25-en>). Extrait : « *The National Telecommunications and Information Administration ("NTIA") has authorized IANA to transition from its current status under USC/ISI to a nonprofit corporation. ICANN has been formed as a nonprofit corporation with a board of directors representing the spectrum of Internet interests around the world to assume the functions previously performed by USC's IANA project. The NTIA has accepted a proposal pursuant to which ICANN will assume the IANA functions* ».

control. To the extent that users decided they should no longer direct their DNS queries in the direction of the legacy root, the contents of the ICANN-controlled root zone file would be irrelevant »¹²⁵. Jon Postel l'avait démontré : techniquement, rien n'interdisait un « coup d'État » contre le registre central existant. Pour ne rien arranger, les premiers membres du conseil d'administration furent désignés selon une procédure opaque, et cultivaient un certain goût du secret qui ne pouvait que déplaire aux acteurs habitués à traiter avec des chercheurs¹²⁶.

Malgré ces défauts, l'organisation a réussi à s'imposer, à la fois parce qu'une alternative sérieuse n'a jamais existé, et parce que les acteurs les puissants d'Internet, qui sont des grandes sociétés américaines, sont parfaitement en mesure d'organiser leur représentation et la prise en compte de leurs intérêts dans la *multistakeholder policy* de l'ICANN. Néanmoins, de nombreux appels à une évolution de la gouvernance de l'association ont été lancés ces dernières années, et ils ont été récemment entendus.

206. La fin de la tutelle du gouvernement américain - Même aux yeux d'un public américain et mondial moins accoutumé que l'opinion publique française à un secteur public fort, « *ICANN's task in seeking public acceptance of its legitimacy was made more complicated by the fact that it was a private entity seeking to play the sort of role more commonly played in our society by public entities* »¹²⁷. Cette situation incongrue est tempérée, si l'on admet la démonstration de M. Weinberg, par le fait que les procédures décisionnelles et de contrôle de l'ICANN ont été conçues sur le modèle des agences fédérales américaines¹²⁸. Le statut d'acteur privé et, surtout, le rôle marginal joué par les États autres que les USA continuent cependant à interroger.

Un véritable événement s'est récemment produit dans l'histoire de l'ICANN, qui a ravivé les débats autour de sa gouvernance : avec la bénédiction de l'administration Obama, le cordon ombilical qui reliait l'organisation au gouvernement américain a été coupé. Après plusieurs renouvellements, le contrat qui les liait a en effet définitivement pris fin le 1er octobre 2016¹²⁹. Le processus avait été initié en 2014. La *National Telecommunications and Information Administration* avait cependant fixé des conditions.

NTIA has communicated to ICANN that the transition proposal must have broad

125. - *Ibid.*, p. 215.

126. - *Ibid.*, p. 212.

127. - *Loc. cit.*

128. - *Ibid.*, p. 225 : « *ICANN has structured its policymaking process so that, in important ways, it looks like a typical U.S. federal administrative agency* ». Cette affirmation est ensuite largement développée.

129. - V. l'annonce par la *National Telecommunications and Information Administration* (NTIA), le jour même : *Statement of assistant secretary Strickling on IANA functions contract*, <https://www.ntia.doc.gov/press-release/2016/statement-assistant-secretary-strickling-iana-functions-contract>.

*community support and address the following four principles: support and enhance the multistakeholder model; maintain the security, stability, and resiliency of the Internet DNS ; meet the needs and expectation of the global customers and partners of the IANA services ; and, maintain the openness of the Internet*¹³⁰.

En insistant sur la nécessité de renforcer le *multistakeholder model*, l'administration américaine repoussait toute velléité de faire basculer le pilotage de l'ICANN dans un paradigme radicalement nouveau. La Russie et la Chine avaient évoqué l'idée de le confier à une organisation internationale inspirée de l'Organisation des Nations Unies¹³¹. Ce projet avait d'ailleurs été dénoncé par un sénateur américain, plusieurs fois candidat à l'élection présidentielle, comme menaçant les intérêts nationaux et la liberté d'expression à travers le monde¹³². Un rapport parlementaire français mentionnait également cette possibilité, mais affirmait sa préférence pour une organisation internationale de droit privé suisse « à personnalité juridique internationale », sur le modèle du Comité international de la Croix-Rouge¹³³. L'ICANN se contenta d'une révision de ses règles internes, dans le but affiché de renforcer ses contre-pouvoirs et d'améliorer la représentation de la « communauté » des parties prenantes dans le bon fonctionnement d'Internet¹³⁴.

La diplomatie française, dans un communiqué officiel, a regretté que la nouvelle organisation réserve à nouveau une place réduite aux États « en comparaison du rôle accordé au secteur privé dont les principaux acteurs sont américains ». Elle regrettait le rôle insuffisant ménagé au *Governmental Advisory Committee*, et appelait l'administration américaine « à accorder la plus grande attention aux préoccupations exprimées par de nombreux États ». Elle annonçait rester attentive aux nécessaires améliorations de l'ICANN, « notamment concernant le renforcement de la diversité géographique et la lutte contre les conflits d'intérêts »¹³⁵.

130. - NTIA, *NTIA announces intent to transition key internet domain name functions*, 14 mars 2014 : <https://www.ntia.doc.gov/press-release/2014/ntia-announces-intent-transition-key-internet-domain-name-functions>.

131. - G. Pépin, « Le plan de l'ICANN pour s'émanciper des États-Unis », article nextinpact du 14 août 2015.

132. - W. Gardner Selby, « Ted Cruz incorrect about Obama giving control of internet to UN-like body », article *politifact.com* du 14 septembre 2016, incluant la vidéo de M. Cruz prenant la parole quelques jours plus tôt devant le Sénat américain pour déclarer : « *If Congress fails to act, the Obama administration intends to give away control of the internet to an international body akin to the United Nations* ».

133. - C. Morin-Desailly, *L'Europe au secours de l'Internet : démocratiser la gouvernance de l'Internet en s'appuyant sur une ambition politique et industrielle européenne*, Rapport d'information du Sénat n° 696 fait au nom de la Mission commune d'information sur la gouvernance mondiale de l'Internet, déposé le 8 juillet 2014.

134. - ICANN, *Revised ICANN bylaws and restated articles of incorporation* : <https://www.icann.org/en/stewardship-implementation/amending-icann-s-bylaws>.

135. - France Diplomatie, *Gouvernance de l'Internet - réforme de l'ICANN*, publication du 10 mars 2016 : <http://www.diplomatie.gouv.fr/fr/politique-et-rangere-de-la-france/diplomatie-numerique/evenements/article/gouvernance-de-l-internet-reforme-de-l-icann-10-03-16>.

À l'inverse, les grandes sociétés américaines du numérique ne cachent pas leur satisfaction¹³⁶.

207. La propriété des infrastructures : bilan - En droit français, il y a longtemps que la propriété privée n'est plus analysée — si elle l'a jamais été — comme un droit absolu, abandonné à l'égoïsme sans frein de son titulaire, exercé dans l'ignorance ou l'incurie du reste du monde. Le droit de propriété s'insère dans une organisation sociale bien plus vaste, qui lui confère son sens et lui assigne ses limites.

L'étude des principales infrastructures physiques nécessaires au fonctionnement d'Internet a fourni des illustrations particulièrement frappantes de situations dans lesquelles une gouvernance collective des propriétés individuelles est incontournable. Les réseaux de télécommunications doivent notamment leur valeur au développement d'un Internet mondial souple et ouvert à l'innovation. Si chaque propriétaire de réseau considère son intérêt personnel de court terme, il peut être tenté d'imposer une discrimination des contenus, certains étant ralentis ou tout bonnement empêchés de circuler, tandis que d'autres sont promus, accélérés au nom d'une meilleure « qualité de service ». Le risque collectif est grand d'étouffer la créativité, de museler la concurrence, d'empêcher le libre discours. À moyen terme, cela revient à tarir la source à laquelle on s'abreuve. Il est alors de la responsabilité du législateur de raviver la flamme de l'intérêt général. S'agissant de l'attribution des IP et domaines, elles peuvent s'analyser comme de simples entrées dans un annuaire mondial, lui-même constitué de serveurs faisant l'objet de droits de propriété privée. Par le jeu d'un système pyramidal, le bon fonctionnement d'un titanesque réseau global est suspendu à quelques ordinateurs appartenant une association à but non lucratif de droit californien. Pour s'assurer que le droit de propriété est assuré à bon escient, c'est à la gouvernance de cette structure qui faut s'attacher.

À ces deux problèmes juridiques différents, deux réponses différentes devaient nécessairement être apportées.

Dans le cas des réseaux de télécommunications, les titulaires du droit de propriété importent peu : ce qui compte, ce sont les limites qu'il convient de fixer à leur jouissance exclusive. Il était donc nécessaire d'imposer la neutralité du net par le haut - par le législateur national ou européen, ou encore par une autorité administrative comme la FCC sur la base du droit préexistant. Les sujétions ainsi imposées constituent des formes de servitudes d'intérêt public. Un résultat plutôt

136. - Internet association, *An open letter to Congress from U.S. Business* : « [...] we congratulate those who worked tirelessly to develop the proposal and we celebrate the effort that will enshrine America's commitment to ensuring the future of a global, interoperable and stable global Internet » : <https://cdn1.internetassociation.org/wp-content/uploads/2016/04/Open-Letter-Supporting-IANA-Transition-041916.pdf>. Sous le texte, figurent les logos d'Intel, Amazon, Microsoft, Hewlett Packard, Dell, Cisco...

convaincant avait été obtenu, jusqu'au récent revirement américain, qui menace l'ensemble de l'édifice d'écroulement. Dans le cas des serveurs DNS, les ressources qui doivent être gérées dans l'intérêt général ne sont pas cette fois-ci nombreuses et décentralisées, mais au contraire uniques et concentrées dans les mains d'une seule personne juridique. La question primordiale est alors celle de l'identité du titulaire du droit de propriété et, corrélativement, de sa capacité à représenter l'ensemble des intérêts composites qui se retrouvent pour souhaiter le bon fonctionnement du réseau global. L'intérêt général se construit ici par le bas. Les solutions pour coordonner les IP et domaines au niveau mondial ont en effet été bâties, à l'origine, par quelques chercheurs au plus près du terrain. Lorsqu'il s'est agi d'élargir la palette des communautés représentées, le choix d'une structure de droit international public a échoué à s'imposer, au profit du maintien d'une personne morale de droit privé à caractère non lucratif. Sa représentativité est imparfaite - comme l'est celle de toute démocratie indirecte, ou celle des sociétés commerciales, et plus généralement de toute organisation politique. Les grands acteurs privés américains y disposent d'un poids considérable, qui n'est toutefois que le reflet de leur importance dans la société numérique contemporaine. S'il faut continuer à observer le fonctionnement de l'ICANN avec vigilance, il ne semble actuellement ni favoriser ni marginaliser brutalement quelque acteur que ce soit¹³⁷. Il est loisible à tout un chacun de se voir affecter une adresse IP, ou d'acheter un nom de domaine pour quelques euros. L'intérêt collectif à ce que le système fonctionne bien est une réalité, et constitue sans doute la meilleure des garanties.

Dans ces deux exemples, des techniques juridiques radicalement différentes ont été employées pour préserver une ressource commune. Les « communs » désignent peut-être moins des moyens qu'une fin : dépasser l'exercice égoïste de la propriété privée, dans l'espoir de conserver une valeur qui pourrait sans cela disparaître. Mais, en ce qui concerne les réseaux de télécommunications, plusieurs acteurs ont prétendu qu'à trop favoriser l'intérêt général, le risque est d'exercer une contrainte excessive sur les propriétaires, qui sont alors découragés d'acheter ou d'investir, ce qui est une autre manière de mettre la ressource commune en danger.

Cet affrontement entre intérêts privés et intérêt général se retrouvera dans l'étude de la couche des contenus.

137. - Comp. avec le brusque départ de l'*Electronic Frontier Foundation* du comité W3C, organisme de standardisation visant notamment à l'harmonisation du HTML. L'EFF proteste contre l'inclusion de technologies de DRM dans l'HTML5. L'EFF estime que la méthode de décision par consensus n'y fonctionne plus : « [...] In essence, a core of EME proponents was able to impose its will on the Consortium, over the wishes of a sizeable group of objectors — and every person who uses the web » (C. Doctorow, « An open letter to the W3C Director, CEO, team and membership », article *eff.org* du 18 septembre 2017).

Section 2 - Les contenus

208. **Les créations de l'esprit, propriétés atypiques** - Il vient d'être rappelé qu'Internet est d'abord constitué d'un ensemble d'infrastructures complexes, qui servent à transporter l'information et à coordonner sa circulation. Mais la plomberie la plus sophistiquée du monde n'est d'aucun intérêt sans fluide à distribuer. Certes, une petite partie des contenus est constituée d'échanges anodins entre utilisateurs, dont le droit tient compte en tant qu'il protège la liberté du discours, mais qu'il ne cherche pas à appréhender comme des richesses. L'essentiel des informations qui donnent vie au réseau des réseaux est cependant fait de véritables créations de l'esprit : textes, images, sons, créations multimédias de toutes sortes, œuvre d'amateurs ou de professionnels, dont l'originalité est suffisante pour prétendre à la protection du droit de la propriété littéraire et artistique en général, et du droit d'auteur en particulier¹³⁸.

Certains cherchent à minorer l'originalité des actifs culturels : il conviendrait d'y appliquer les règles ordinaires de la propriété. Ainsi le président de la Motion Pictures Association of America a-t-il pu déclarer devant le Congrès :

*No matter the lengthy arguments made, no matter the charges and the counter-charges, no matter the tumult and the shouting, reasonable men and women will keep returning to the fundamental issue, the central theme which animates this entire debate: Creative property owners must be accorded the same rights and protection resident in all other property owners in the nation. That is the issue. That is the question*¹³⁹.

Placés le temps d'un discours dans des situations prétendument identiques, les titulaires d'un droit sur des œuvres de l'esprit devraient alors de voir reconnaître des prérogatives aussi puissantes, par exemple, que celles d'un propriétaire immobilier sur son fonds. Mais l'analogie a ses limites, et le droit d'auteur ses spécificités¹⁴⁰.

138. - M. Vivant et J.-M. Bruguière, *Droit d'auteur et droits voisins*, Dalloz, précis, 3e éd., 2016, n° 257 : « L'originalité est considérée — et à juste titre — comme la “pierre angulaire” du droit d'auteur, le critère qui finalement fait reconnaître ou refuser la protection à une œuvre, au point, d'ailleurs, que certains [...] en font même un élément de définition de l'œuvre. Explicite ou implicite, elle est présente dans tous les systèmes juridiques, quitte à ce que l'unicité du vocable recouvre des disparités de compréhension ».

139. - Jack Valenti, témoignage devant le Congrès en 1982, cité par L. Lessig, *Free Culture*, The Penguin Press, 2004, p. 117. L'ouvrage est consultable à l'adresse : <http://www.free-culture.cc/freeculture.pdf>.

140. - Certes, le Conseil constitutionnel lui-même décide : « Considérant que les finalités et les conditions d'exercice du droit de propriété ont subi depuis 1789 une évolution caractérisée par une extension de son champ d'application à des domaines nouveaux ; que, parmi ces derniers, figurent les droits de propriété intellectuelle et notamment le droit d'auteur et les droits voisins » (décision n° 2006-540, considérant 15). Notre étude traite elle-même la propriété intellectuelle comme se rattachant à un concept plus général du droit privé, qui est celui de propriété. Cela n'empêche pas de la doter de règles dérogatoires, à raison de la spécificité de son objet.

L'une des premières différences généralement relevées consiste dans l'immatérialité des biens concernés :

[...] le fait que le droit d'auteur relève de l'immatériel est fondamental. Tout d'abord, il coexiste avec toutes les manifestations de l'immatérialité dans le droit : les objets de droit de propriété intellectuelle bien évidemment, mais aussi les créances, les clientèles, les valeurs mobilières ou les informations. Cette énumération prouve que le droit d'auteur appartient à cette grande immatérialité qui, de nos jours, fédère les plus importantes richesses¹⁴¹.

Pour fondamentale qu'elle soit, cette immatérialité n'est peut-être pas la caractéristique la plus marquante des actifs culturels. Prenons l'exemple d'une part sociale. Est-il si important qu'elle soit incorporée dans un morceau de papier, ou qu'elle soit dématérialisée et prenne l'aspect d'une simple écriture sur un compte ? Bien sûr, des règles relatives à la possession, à la cession, à la preuve du droit peuvent s'en trouver modifiées. Mais il s'agit dans les deux cas d'organiser un tête-à-tête entre le propriétaire et sa chose, dans lequel l'immixtion de tiers — par démembrement de la propriété, ou par l'exercice d'une propriété collective — sera rare et d'ampleur limitée. L'argent lui-même est devenu largement immatériel. Le client qui règle sa dette à la caisse d'un magasin n'a pas le sentiment de réaliser un geste substantiellement différent, selon qu'il use d'espèces — qui sont des biens matériels — ou qu'il déclenche des mouvements de monnaie scripturale immatérielle à l'aide de sa carte bancaire.

Cela s'explique sans doute par l'appartenance des parts sociales immatérielles ou de la monnaie scripturale à la catégorie des biens rivaux, tandis que l'information est un bien non-rival : « l'utilisation, la consommation du bien par un agent économique ne retire aucune utilité à ce bien qui peut également être consommé par un autre agent. Un savoir partagé reste un égal savoir et un poème peut être connu par deux personnes sans que l'une ou l'autre en pâtisse »¹⁴². Il y a moins de distance entre la propriété d'une créance dématérialisée et celle d'un réseau de télécommunications ou des serveurs de l'ICANN, tous biens rivaux, qu'entre la propriété d'une telle créance et celle d'un roman. Le bien rival est voué à ne profiter qu'à un seul ou, au mieux, à un groupe restreint ; le bien non-rival pourrait profiter à tous. Le droit de propriété du premier aménage une rareté matérielle indépassable. Le droit de propriété du second fait surgir de la loi et de la technique une rareté artificielle et finalisée : « Permettre d'exclure les tiers de l'usage du bien ou de tel ou tel usage autorise ainsi des transactions, ce qui conduit à définir des prix et donc bien à donner une

141. - C. Caron, *Droit d'auteur et droits voisins*, Litec, 4e éd., 2015, n° 19.

142. - M. Vivant et J.-M. Bruguière, *op. cit.*, n° 5.

valeur marchande au bien. Ainsi le droit des biens d'instance juridique *crée cette valeur* en permettant de faire de l'objet immatériel un objet d'échange »¹⁴³.

Sans les protections érigées par le droit de propriété, le bien rival n'en serait pas moins réservé à l'usage d'un seul - qui serait simplement, alors, le plus fort ou le plus retors. En revanche, s'il n'était dissimulé derrière une abstraction juridique, d'où il sort ponctuellement pour offrir son usage à ceux capables de payer et disposés à le faire, le bien non rival profiterait à tous. Le fonds culturel commun s'étendrait, dans lequel chacun pourrait puiser pour s'en imprégner, et pour créer à son tour sur sa base, sans jamais risquer de l'assécher. La tension entre l'intérêt particulier du propriétaire et l'intérêt général, si elle existe s'agissant des biens rivaux — que l'on songe aux développements précédents sur la neutralité du réseau — prend donc une physionomie très particulière en matière d'information. L'ensemble de ces considérations explique aisément la différence la plus spectaculaire entre le droit de propriété classique, qui est imprescriptible, et le droit d'auteur, qui constitue un monopole d'exploitation de l'œuvre d'une durée limitée : actuellement, pour la vie du créateur prolongée de soixante-dix années¹⁴⁴.

209. La pression exercée sur le droit d'auteur par le numérique - Si l'influence du numérique sur le droit d'auteur se traduit par une multitude de problèmes techniques et d'ajustements conceptuels — dont il ne sera donné ici qu'un très modeste aperçu -, le mouvement général est facile à appréhender. Les murailles dressées autour de l'œuvre, bien non rival qui ne demande qu'à s'en échapper, sont fragiles. Techniquement, le numérique n'est rien d'autre que la capacité à produire des copies d'un ensemble d'informations qui sont à la fois parfaites, peu coûteuses et quasiment instantanées. La capacité des titulaires de droits à empêcher les proliférations non autorisées a donc commencé par s'écrouler. Mais un phénomène inverse et plus récent doit être relevé : une fois domestiqué, le numérique s'est mué en un canal de distribution des richesses culturelles offrant à celui qui en a la maîtrise un degré de contrôle sans précédent. La consommation d'œuvres, un temps présentée comme gangrénée par les usages illégaux et gratuits, fait aujourd'hui l'objet d'un encadrement parfois excessif. Un déséquilibre chasse l'autre. Ainsi, après avoir consacré l'essentiel de l'étude aux contours du droit sur les œuvres (I), il faudra évoquer plus brièvement le droit des acheteurs sur les copies d'œuvres (II) : la propriété affronte la propriété.

143. - *Ibid.*

144. - Article L. 123-1 du Code de la propriété intellectuelle.

I - Le droit sur les œuvres

210. **Plan** - Le geste créatif a bien des ressorts. L'appât du gain — ou, plus modestement, l'envie de vivre de sa production — en est un. Il sera souvent secondaire, ou même absent des motivations de l'auteur ou de l'artiste : l'obéissance à une aspiration profonde, le plaisir, la recherche de gratifications de nature symbolique expliquent alors la démarche¹⁴⁵. Mais à l'inverse, la possibilité de monnayer l'accès à ces créations se révèle parfois primordiale. D'abord, lorsqu'elle permet au créateur de vivre de son droit d'auteur - ce qui renvoie à un petit nombre d'individus, qui se spécialisent et font profession de nourrir les esprits de leurs semblables. Ensuite, lorsque l'on considère l'écosystème économique qui gravite autour de la création, autrement dit « l'industrie culturelle » avec ses intermédiaires spécialisés, ses éditeurs, ses producteurs, ses studios : autant d'acteurs qui n'investiront du temps, des compétences et de l'argent dans la sélection, la promotion et la diffusion des biens culturels que pour autant qu'ils ont la possibilité juridique de protéger leur « investissement »¹⁴⁶. En droit français, il s'est donc agi avant tout de préserver l'édifice constitué par la propriété littéraire et artistique face aux bouleversements induits par le numérique, et même d'exploiter certaines possibilités offertes par les nouvelles technologies pour renforcer le contrôle de la distribution des biens culturels (A). Toutefois, l'intérêt général à une large diffusion des connaissances et divertissements n'est pas ignoré. Des relâchements de l'auteur et de ses ayants droit sur les œuvres peuvent survenir, soit que la loi l'ordonne, soit que la volonté y consente (B).

A - La propriété protégée

211. **Plan** - La propriété littéraire et artistique a non seulement plutôt bien résisté aux assauts de la numérisation, mais elle s'est même livrée à une surprenante contre-attaque, étendant à certains égards son empire. Après avoir constitué sinon une menace, du moins un facteur de bouleversement (1), le numérique constitue aujourd'hui une opportunité (2).

1. - La résistance au numérique

212. **Plan** - La plus grande menace que constitue le numérique pour la propriété littéraire et artistique, c'est la possibilité donnée aux internautes de faire circuler les œuvres, avec une

145. - M. Vivant et J.-M. Bruguère, *op. cit.*, n° 7 : « [...] le peintre qui brosse sa toile seul dans son atelier créera sans considération de ce que lui offre ce droit. Il est des œuvres qui naissent parce que l'auteur sent le besoin irrépressible de créer. Le cadre juridique ne fait rien à l'affaire ».

146. - V. par exemple les chiffres cités dans T. Picard, « Le poids économique direct de la culture en 2015 », *Cultures-chiffres*, 2017, n° 1, consultable sur www.culturecommunication.gouv.fr. Ce poids était de 43 milliards d'euros en 2015.

déconcertante facilité, hors du contrôle du titulaire du droit d'auteur ou du droit voisin, en violation de son droit patrimonial, voire de son droit moral¹⁴⁷. Mais il convient de distinguer deux situations bien différentes. Celle, d'abord, dans laquelle l'œuvre est arrachée à son artificielle rareté pour être répandue aux quatre vents, sans avoir été ni améliorée ni altérée (a). Celle, ensuite, dans laquelle l'œuvre ne circule qu'en accessoire ou en arrière-plan d'une création nouvelle, parce qu'elle a servi de base à un détournement, une réinterprétation, une reconstruction, toutes pratiques qui n'ont pas été inventées par le numérique, mais grandement facilitées par lui (b).

a – La circulation non transformative

213. **La reproduction** - Le titulaire du droit d'auteur jouit d'un monopole lorsqu'il s'agit de reproduire son œuvre. Aux termes du Code de la propriété intellectuelle, la reproduction consiste « dans la fixation matérielle de l'œuvre par tous procédés qui permettent de la communiquer au public d'une manière indirecte »¹⁴⁸. Pour autant, l'auteur ou son ayant droit ne peut interdire « Les copies ou reproductions réalisées à partir d'une source licite et strictement réservées à l'usage privé du copiste et non destinées à une utilisation collective » - ce que l'on appelle « les copies privées »¹⁴⁹. Or, le numérique permettant de réaliser des copies quasiment gratuites et presque instantanées, on a pu craindre qu'un seul exemplaire d'un CD audio, d'un film, d'un jeu vidéo soit acquis avant d'être copié dans tout le cercle amical et familial de l'acheteur, ce qui aurait nui aux ventes d'œuvres. Deux réponses complémentaires ont été abordées.

D'abord, une « rémunération pour copie privée » est prévue par le Code pour compenser ces pertes supposées¹⁵⁰. L'argent est issu d'une redevance perçue sur les supports susceptibles d'être employés pour enregistrer des œuvres : CD vierges, clés USB, cartes mémoires, disques durs externes, tablettes¹⁵¹...

Ensuite et surtout, la Cour de cassation a jugé que la possibilité de réaliser une copie privée ne constitue pas un droit, mais une simple exception, susceptible d'être empêché par des mesures techniques de protection (MTP) si cela est nécessaire « au regard des risques inhérents au nouvel

147. - Sur l'ensemble de ces questions : V. Varnerot, « La circulation des œuvres numériques » in *Les biens numériques*, éd. Ceprisca, 2014, p. 109.

148. - Article L. 122-3 CPI.

149. - Article L. 122-5 CPI.

150. - Article L. 311-1 CPI : « Les auteurs et les artistes-interprètes des œuvres fixées sur phonogrammes ou vidéogrammes, ainsi que les producteurs de ces phonogrammes ou vidéogrammes, ont droit à une rémunération au titre de la reproduction desdites œuvres, réalisée à partir d'une source licite dans les conditions mentionnées au 2° de l'article L. 122-5 et au 2° de l'article L. 211-3 [...] ».

151. - Article L. 311-4 CPI. Pour une liste des supports taxés, V. le site copiefrance.fr.

environnement numérique quant à la sauvegarde des droits d'auteur [...]»¹⁵². L'essor de ces MTP — sur lequel nous reviendrons ultérieurement — est suffisant pour que la copie privée soit vraisemblablement cantonnée, à l'avenir, à un épiphénomène incapable de remettre en question l'efficacité du droit patrimonial de l'auteur¹⁵³.

Aux États-Unis, un mélange similaire de redevances pour copie privée et de MTP avait été mis en place, dès 1992, avec le *Audio Home Recording Act* : « *The Audio Home Recording Act both taxed blank tapes slightly and regulated the code of digital reproduction technologies directly. The Act requires producers of digital recording devices to install a chip in their systems that implements a code-based system to monitor the copies of any copy made on that machine. The chip would allow a limited number of personal copies, but on copies of copies, the quality of the recording would be degraded* »¹⁵⁴.

Ainsi, la capacité de l'exception de copie privée à nuire aux intérêts de l'auteur n'a pas augmenté à la faveur de l'apparition des procédés numériques. C'est même l'inverse qui s'est produit : toujours en vigueur juridiquement, cette exception est menacée de s'éteindre un jour dans les faits. Le choc en retour est remarquable.

214. La représentation - Le titulaire du droit d'auteur jouit encore d'un droit exclusif de représentation, définie comme « [...] la communication de l'œuvre au public par un procédé quelconque [...] »¹⁵⁵. Deux moyens de communication propres au numérique méritent une attention particulière : l'échange de fichiers sur un réseau de pair-à-pair, et l'utilisation d'un lien hypertexte pointant vers une page représentant l'œuvre.

215. Les réseaux de pair-à-pair - Ces réseaux permettent une distribution décentralisée de fichiers directement entre utilisateurs. On aurait tort d'assimiler entièrement ces techniques à une violation systématique de droits de propriété intellectuelle : on y trouve des fichiers dont le contenu n'est pas protégé par la propriété littéraire et artistique, de même que des œuvres tombées dans le domaine public, ou encore placées sous une licence libre - notion qui sera abordée ultérieurement¹⁵⁶.

152. - Affaire dite « Mulholland drive » - Cass. 1ère civ., 28 février 2006, n° 05-15.824 et 05-16.002 : RTD. com., 2007, p. 357, obs. F. Pollaud-Dulian ; CCE, 2006, comm. 56, note C. Caron ; JCP G, 2006, p. 1065, note A. Lucas ; Gaz. Pal., 5 mars 2006, n° 64, p. 6, avis de l'avocat général D. Sarcelet.

153. - Pour éviter que les consommateurs ne soient pénalisés à la fois par une redevance et par l'impossibilité technique de réaliser des copies privées, l'article L. 311-4 CPI prévoit in fine : « Le montant de la rémunération tient compte du degré d'utilisation des mesures techniques définies à l'article L. 331-5 et de leur incidence sur les usages relevant de l'exception pour copie privée [...] ».

154. - L. Lessig, *Code V2*, op. cit., p. 115. Le *Audio Home Recording Act* est consultable à l'adresse : <https://www.gpo.gov/fdsys/pkg/STATUTE-106/pdf/STATUTE-106-Pg4237.pdf>.

155. - Article L. 122-2 CPI.

156. - Sur le caractère « neutre » de ces techniques : A. Bensamoun et J. Groffe, « Création numérique », in

Mais il est indéniable que l'on y rencontre également nombre d'œuvres protégées. Les logiciels actuels sont ainsi conçus que, dès lors qu'un internaute à la recherche d'un fichier parvient à se procurer un premier fragment auprès d'un pair, il le met lui-même automatiquement à la disposition de tout intéressé. Ce mode de fonctionnement rend la licéité de l'opération plus simple à appréhender. S'il s'était agi uniquement de prendre sans rien donner — de *download* sans *upload* —, la question aurait pu se poser du recours à l'exception de copie privée, revivifiée pour l'occasion, encore que, depuis 2011, l'exception soit cantonnée à la reproduction d'une copie « licite » - qualité douteuse dans un tel contexte¹⁵⁷. Mais puisque l'internaute est obligé de mettre son fichier ou fragment à disposition de tout utilisateur intéressé du même réseau, il n'y a guère de doute qu'il réalise une communication au public, illicite¹⁵⁸.

La question de la qualification juridique est ici facilement résolue, mais c'est la question de la juste sanction qui cristallise les difficultés. Si le recours aux sanctions civiles de la violation du monopole de l'auteur pouvait sembler insuffisant aux ayants droit, la mise en œuvre du droit pénal apparaissait d'une sévérité excessive. La contrefaçon, en tant qu'elle constitue un délit, est actuellement punie de trois ans d'emprisonnement et 300 000 euros d'amende¹⁵⁹. Or, en 2009, 45% des internautes se connectant quotidiennement ont déclaré « télécharger ou utiliser des contenus téléchargés illégalement »¹⁶⁰. Quoiqu'illégale, la pratique fait donc l'objet d'une large acceptation sociale, qui rend difficilement envisageables des amendes en dizaines ou centaines de milliers d'euros, a *fortiori* le prononcé de peines de prison, même assorties du sursis. Des auteurs interrogent : « n'y a-t-il pas une différence entre le contrefacteur des pièces d'une voiture ou de médicaments et l'internaute qui télécharge le dernier album de U2 ? »¹⁶¹. Ils reconnaissent que la loi pénale ne distingue certes pas entre le vol de pomme et le vol de bijoux : il s'agit toujours d'un vol, et le pouvoir conféré au juge pénal de personnaliser la sanction permet de traiter différemment des situations différentes. Mais ils se demandent si, s'agissant de la contrefaçon, l'hétérogénéité des

Rép. civ. Dalloz, juin 2014, n° 166. Sur les procès intentés aux USA contre les éditeurs des logiciels d'échanges : P. Sirinelli, « Le peer-to-peer devant la Cour suprême », *D.*, 2005, p. 1796. La licéité de l'outil n'y a pas été remise en cause en elle-même.

157. - Article L. 122-5 CPI, précité. M. Vivant et J.-M. Bruguière tentent tout de même de pousser le raisonnement jusqu'au bout : *op. cit.*, n° 626.

158. - V. par ex. les décisions de juridictions du fond citées par J. Francillon, « Piratage numérique », *RSC*, 2006, 93.

159. - Art. L. 335-2 CPI.

160. - TNS SOFRES pour Métro, « Les français et le téléchargement illégal sur internet », 2009, sondage cité par M. Dalle, « Réflexions sur l'éducation des internautes au respect du droit d'auteur », in *Les biens numériques*, éd. Ceprisca, 2015, p. 89.

161. - M. Vivant et J.M. Bruguière, *op. cit.*, n° 1092.

pratiques visées n'est pas telle qu'elle mérite, *de lege ferenda*, de scinder l'infraction en plusieurs parties¹⁶².

Le législateur, par le passé, a exploré cette voie. La loi du 1er août 2006, dite « DADVSI », prévoyait une incrimination spécifique pour la contrefaçon commise par un échange sur un réseau de pair-à-pair, punie d'une simple contravention¹⁶³. Le Conseil constitutionnel a cependant considéré que :

[...] au regard de l'atteinte portée au droit d'auteur ou aux droits voisins, les personnes qui se livrent, à des fins personnelles, à la reproduction non autorisée ou à la communication au public d'objets protégés au titre de ces droits sont placées dans la même situation, qu'elles utilisent un logiciel d'échange de pair-à-pair ou d'autres services de communication au public en ligne ; que les particularités des réseaux d'échange de pair-à-pair ne permettent pas de justifier la différence de traitement qu'instaure la disposition contestée [...].

Le Parlement trouva ultérieurement la solution, ainsi qu'il a déjà été exposé. Il suffit de punir le titulaire d'un abonnement à Internet pour n'avoir pas surveillé correctement son accès au réseau, de sorte qu'il a servi à une contrefaçon en ligne¹⁶⁴. Cette idée résout deux problèmes distincts à elle seule. Le premier : parmi les différentes personnes capables d'utiliser le point d'accès au réseau, avec ou sans l'autorisation du titulaire, il est très difficile de savoir à qui imputer la violation du droit d'auteur. Or, la loi pénale ne s'accommode ni des incertitudes ni des punitions collectives. L'infraction ainsi définie vise une personne déterminée. Le deuxième : en incriminant spécifiquement un comportement situé en amont de la contrefaçon en ligne, on parvient sans le dire à isoler cette forme spécifique de violation du droit d'auteur, et à lui attacher une sanction pénale plus clémentielle. La solution est ingénieuse, à défaut d'être simple. Les manquements peuvent être punis d'une contravention de cinquième classe, et d'une suspension provisoire d'accès à Internet¹⁶⁵. Cette dernière sanction devait initialement être prononcée par la Haute Autorité pour la diffusion des œuvres et la protection des droits sur Internet (HADOPI) elle-même ; le Conseil constitutionnel a exigé qu'elle fasse l'objet d'une décision judiciaire¹⁶⁶. Avant d'en arriver là, la Haute autorité aura

162. - *Ibid.*, spéc. note 3 p. 950, où les auteurs invitent à « repenser nos catégories ».

163. - Article 24 de la loi n° 2006-961 du 1 août 2006 relative au droit d'auteur et aux droits voisins dans la société de l'information (censuré).

164. - V. *supra*, n°51.

165. - Sur la contravention : art. R335-5 CPI. Sur la suspension d'accès à internet : art. L. 336-3 al. 2 CPI, par renvoi. Pour une analyse critique de ces sanctions, V. par ex. N. Catelan, « La protection pénale du droit d'auteur : une négligence caractérisée ? », *RLDI*, 2001, n° 67.

166. - V. *supra*, n°119.

toutefois adressé à la personne concernée un certain nombre d'avertissements, dans le cadre d'une procédure dite « de riposte graduée »¹⁶⁷.

Les derniers « chiffres clés de la réponse graduée » font état, entre le 1er septembre 2010 et le 31 janvier 2017, de plus de 8 millions de « 1res recommandations », près de 740 000 « 2e recommandations », un peu moins de 6000 « constats de négligences caractérisées » et environ 1500 transmissions au parquet. 340 « suites judiciaires » ont été recensées, dont environ 20% de classements sans suite, contre près de 80% de « réponses pénales », parmi lesquelles on trouve enfin une majorité de mesures alternatives aux poursuites, le reste étant constitué d'amendes dont le montant est compris entre 500 et 1000 euros¹⁶⁸. Cette pyramide inversée peut être interprétée de diverses manières. Le faible nombre de condamnations issues de cette imposante machine administrative est-il le signe de son impuissance, ou au contraire de sa capacité à dissuader les internautes, à l'issue des premiers avertissements, de poursuivre leurs activités illicites ? Les auteurs relèvent en tout cas l'existence d'alternatives techniques à l'échange de pair-à-pair, qui permettent la contrefaçon hors du regard des agents assermentés par l'HADOPI : *newsgroups*, *streaming*, téléchargement direct, *seedboxes*¹⁶⁹. Par définition, le chiffre noir de ces utilisations est inaccessible. Il est probable que le développement des offres légales — dont la HADOPI rappelle l'existence dans ses messages d'avertissement¹⁷⁰ — jouera un rôle, dans l'infléchissement des pratiques, égal ou supérieur à celui de la répression. En particulier, le développement d'offres à prix mensuel forfaitaire, lorsque les catalogues sont fournis, rapproche l'internaute du vieux rêve de la « licence globale »¹⁷¹.

Quoi qu'il en soit, le constat est clair : le droit d'auteur s'arme pour résister aux usages numériques susceptibles de le miner. Il assouplit ses sanctions au besoin. Il plie, mais ne rompt pas.

Le partage de liens hypertexte menant vers des œuvres sous droit constitue un autre défi.

167. - Art. L. 331-25 CPI. Pour une présentation détaillée de la « riposte graduée », V. par ex. M. Dalle, « Réflexions sur l'éducation des internautes... », art. préc.

168. - HADOPI, *Bulletin d'information trimestriel n° 2 - chiffres clés de la réponse graduée*, février 2017, consultable sur www.hadopi.fr.

169. - Sur les *newsgroups* : F. Chopin, « Téléchargement illégal et Hadopi », *AJ pénal*, 2012, 528. Sur le *streaming* : M. Vivant et J.-M. Bruguière, *op. cit.*, n° 1096. Sur le téléchargement direct et les *seedboxes*, V. l'intervention de la députée I. Attard, en 2013 : M. Rees, « La réponse graduée sera bien transférée au CSA, assure Aurélie Filipetti », article *Nextinpact* du 6 novembre 2013. De manière générale, V. encore le scepticisme de C. Geiger, « HADOPI, ou quand la répression devient pédagogique », *D.*, 2011, p. 773.

170. - La HADOPI est d'ailleurs investie par la loi d'une « mission d'encouragement au développement de l'offre légale » par l'article L. 331-23 CPI.

171. - On songe ici aux célèbres Netflix et autres Canalplay. Le prix d'une diffusion « à la demande » sont encore très élevés : l'exemple de mytf1vod.tf1.fr, pris au hasard, révèle un prix de location en HD de 6 euros. Une famille qui aurait recours à ces solutions un soir sur deux devrait déboursier 90 euros par mois.

216. Hyperliens et droit d'auteur : présentation - Lorsque nous avons traité des communications électroniques, la question du sens profond que revêt la pose d'un lien hypertexte avait déjà été posée¹⁷². En pointant vers un message, suis-je en train de le répéter, ou de proposer une simple note de bas de page électronique tout à fait neutre ? Lier une page diffamatoire revient-il à diffamer ? L'hyperlien suscite également des difficultés en matière de propriété intellectuelle. D'un point de vue rigoureusement technique, elles sont distinctes. D'un point de vue plus fondamental, elles sont en vérité du même ordre : en liant un contenu cible, objet de propriété littéraire et artistique, suis-je en train de le dire, de le montrer, de le jouer : en un mot, de le *représenter*, c'est-à-dire d'activer une prérogative relevant du monopole de l'auteur ? On songe immédiatement à la responsabilité qui pourrait peser sur celui qui crée un lien vers une représentation première elle-même non autorisée. Est-elle envisageable par principe, ou faut-il que l'illicéité ait été connue du poseur de lien, et dans ce cas comment faut-il démontrer cette connaissance ? Mais surgit ensuite une autre question : quand bien même une œuvre aurait été diffusée sur une première page avec toutes les autorisations nécessaires, pointer vers cette page revient-il à proposer une représentation de l'œuvre sur la page contenant le lien ? Il faudrait alors recueillir l'autorisation des titulaires de droit chaque fois qu'une page cible contenant une image, une musique ou même un texte réunissant les conditions d'une protection par le droit d'auteur - en particulier l'originalité, l'empreinte de la personnalité de l'auteur ; il n'est pas nécessaire en revanche que l'œuvre soit méritante. Avec un tel raisonnement, c'en serait fini des liens hypertextes, qui sont au fondement de cette partie d'Internet qu'on appelle le Web.

La Cour de Justice de l'Union européenne a eu l'occasion de répondre à ces différentes questions par une série d'arrêts, dont nous n'examinerons que les plus récents. L'étroitesse de l'échantillon n'exclut pas la complexité du résultat d'ensemble.

217. Hyperliens et droit d'auteur : la jurisprudence de la CJUE - La notion de communication d'une œuvre au public résulte d'une directive européenne, ce qui fonde la compétence de la CJUE pour en livrer une interprétation uniforme¹⁷³.

172. - V.supra, n° 136 et s.

173. - Directive 2001/29/CE du Parlement européen et du Conseil du 22 mai 2001 sur l'harmonisation de certains aspects du droit d'auteur et des droits voisins dans la société de l'information, article 3 : « Droit de communication d'œuvres au public et droit de mettre à la disposition du public d'autres objets protégés » : « Les États membres prévoient pour les auteurs le droit exclusif d'autoriser ou d'interdire toute communication au public de leurs œuvres, par fil ou sans fil, y compris la mise à la disposition du public de leurs œuvres de manière que chacun puisse y avoir accès de l'endroit et au moment qu'il choisit individuellement ».

À s'en tenir au passé récent, le premier arrêt remarquable a été rendu en 2014, dans une affaire *Svensson*¹⁷⁴. Des journalistes se plaignaient que leurs articles, publiés en libre accès sur le site de leur journal, aient fait l'objet de liens cliquables sur un tiers site Internet. Les requérants prétendaient qu'après avoir cliqué, l'internaute ne pouvait pas comprendre qu'il changeait de site, mais la Cour estime que cela ne ressort pas du dossier. C'est donc la question la plus redoutable des deux, celle de la licéité des liens menant vers une œuvre licitement publiée sur la page source, qui était posée. La Cour répond que « le fait de fournir des liens cliquables vers des œuvres protégées doit être qualifié de “mise à disposition” et, par conséquent, d’“acte de communication” », au sens de la directive¹⁷⁵. Mais c'est une communication « au public » qui doit être caractérisée. Là se situe le cœur du raisonnement.

*Cela étant,[...] pour relever de la notion de «communication au public»[...] encore faut-il qu'une communication, telle que celle en cause dans l'affaire au principal, visant les mêmes œuvres que la communication initiale et ayant été effectuée sur Internet à l'instar de la communication initiale, donc selon le même mode technique, soit adressée à un public nouveau c'est-à-dire à un public n'ayant pas été pris en compte par les titulaires du droit d'auteur, lorsqu'ils ont autorisé la communication initiale au public. En l'occurrence, il doit être constaté que la mise à disposition des œuvres concernées au moyen d'un lien cliquable, telle celle au principal, ne conduit pas à communiquer les œuvres en question à un public nouveau. En effet, le public ciblé par la communication initiale était l'ensemble des visiteurs potentiels du site concerné, car, sachant que l'accès aux œuvres sur ce site n'était soumis à aucune mesure restrictive, tous les internautes pouvaient donc y avoir accès librement*¹⁷⁶.

Ainsi, la première publication avait rendu l'œuvre disponible pour tous. Le lien posé n'a donc pas élargi le public touché. Le raisonnement a été critiqué, en ce qu'un site Internet ciblé par un lien, librement accessible, est certes *potentiellement* consultable par tous, mais dispose en réalité d'un lectorat précis, qui n'est pas nécessairement le même que celui de la page source du lien¹⁷⁷. La remarque est techniquement rigoureuse, mais conduirait à des solutions délicates en opportunité, s'il fallait que le poseur de lien procède à une étude comparative des publics du site auquel il entend renvoyer et du sien - sans parler du fait que leurs lectorats, appréhendés avec suffisamment de finesse, ne se superposent *jamais* parfaitement. Pour finir de présenter l'essentiel du raisonnement de la Cour, il faut encore préciser que si l'œuvre située sur le site cible n'est pas librement accessible — par exemple, parce qu'elle est réservée à des abonnés -, le lien qui parviendrait à la

174. - CJUE, 13 févr. 2014, C-466/12, *Nils Svensson c. Retriever Sverige AB* : D., 2014, 2078, obs. P. Sirinellis ; *ibid.* 2317, obs. J. Larrieu, C. Le Stanc et P. Tréfigny ; *RTD com.*, 2014. 600, obs. F. Pollaud-Dulian ; *RTD eur.*, 2014, 965, obs. E. Treppoz.

175. - §20.

176. - §24 à 26.

177. - Par ex. P. Sirinelli, obs. préc.

livrer au regard de tous constituerait une communication à un public nouveau. Un tel lien relève cependant d'une démarche très particulière : il a sciemment été conçu pour contourner une mesure technique de protection. En résumé, l'arrêt *Svensson*, s'il n'était pas à l'abri de critiques techniques, se révélait protecteur de la liberté de poser un lien vers une œuvre licitement publiée et accessible à tout internaute - ce qui n'est pas un mince acquis.

Quelques mois plus tard, une affaire *Bestwater* posait une question un peu différente¹⁷⁸. Le choix de statuer par ordonnance signifie que la Cour croit pouvoir répondre à la question posée par une simple référence à sa jurisprudence antérieure - en l'occurrence, la jurisprudence *Svensson*. Pourtant, la situation n'était pas tout à fait la même. Dans cette affaire, une vidéo avait été placée sur la plateforme YouTube. Il était allégué que cette première publication avait été réalisée sans l'accord du titulaire du droit d'auteur, mais cette circonstance est totalement ignorée dans le raisonnement de la Cour. En revanche, la difficulté principale tient au fait que la vidéo n'avait pas simplement fait l'objet d'un lien classique, mais d'une « transclusion ». Un lien classique oblige à quitter la page source et ouvre une page cible. La transclusion réalise comme une découpe au sein même de la page source, qui laisse apparaître à travers elle le média lié. L'internaute accède donc à l'œuvre sans quitter la page d'origine. Pour la CJUE, cela ne change rien au raisonnement, à nouveau construit autour de la notion de public nouveau : « En effet, dès lors que et tant que cette œuvre est librement disponible sur le site vers lequel pointe le lien Internet, il doit être considéré que, lorsque les titulaires du droit d'auteur ont autorisé cette communication, ceux-ci ont pris en compte l'ensemble des internautes comme public »¹⁷⁹.

En revanche, lorsqu'elle rendit en 2016 un arrêt *GS Media*, la CJUE ne se contenta pas de répéter la jurisprudence *Svensson* : elle y ajouta, et même elle l'infléchit¹⁸⁰. Cette fois-ci, il s'agissait sans aucune ambiguïté d'aborder le problème d'une publication initiale illicite, que le lien contribue à faire circuler. Des photos d'une célébrité néerlandaise avaient été mises en ligne sans autorisation du photographe. La société GS Media avait placé sur son propre site des hyperliens y conduisant. Avertie du caractère illicite de la publication cible, GS Media n'en tint aucun compte. Pire : au fur et à mesure que les sites cibles retiraient l'œuvre à la suite des démarches entreprises par les

178. - CJUE, ordonnance du 21 octobre 2014, C-348/13, *BestWater International GmbH c. Michael Mebes, Stefan Potsch* : D. 2015, 2214, obs. J. Larrieu, C. Le Stanc et P. Tréfigny ; *RTD com.*, 2014., 808, obs. F. Pollaud-Dulian.

179. - §18.

180. - CJUE, 8 septembre 2016, *GS Media BV c. Sanoma Media Netherlands BV*, C-160/15 : *Dalloz IP/IT*, 2016, p. 543, obs. P. Sirinelli ; *Gaz. Pal.*, 7 février 2017, n° 6, p. 21, obs. L. Marino ; *CCE*, 2017, n° 2, p. 15, obs. S. Dormont ; *RLDI*, 2016, n° 132, p. 8, obs. G. Busseuil ; *Propriétés Intellectuelles*, oct. 2016, n° 61, p. 436, note J.-M. Bruguière ; *RLDI*, 2016, n° 130, p. 12, obs. L. Costes ; *vlbenabou.blog*, note du 15 oct. 2016, obs. V.-L. Benabou.

titulaires des droits, GS Media guettait leur réapparition sur d'autres pages, et les liait aussitôt. Par définition, il n'était plus possible de dédouaner l'auteur du lien au prétexte d'une absence de public nouveau. La page source n'ayant fait l'objet d'aucune autorisation, le public initial (« pris en compte par les titulaires du droit d'auteur ») était inexistant, et le public fédéré par le lien devait par conséquent être automatiquement qualifié de nouveau. Du moins le croyait-on. Il est probable que la CJUE n'est pas émue à l'idée des sanctions qui sont sur le point de s'abattre sur GS Media ; mais les magistrats ont le souci de ne pas motiver leur décision de telle sorte à frapper avec elle le grand public, et les poseurs de liens du dimanche. Ainsi écrivent-ils :

[...] il peut s'avérer difficile, notamment pour des particuliers qui souhaitent placer de tels liens, de vérifier si le site Internet, vers lequel ces derniers sont censés mener, donne accès à des œuvres qui sont protégées et, le cas échéant, si les titulaires des droits d'auteur de ces œuvres ont autorisé leur publication sur Internet. Une telle vérification s'avère d'autant plus difficile lorsque ces droits ont fait l'objet de sous-licences. Par ailleurs, le contenu d'un site Internet, auquel un lien hypertexte permet d'accéder, peut être modifié après la création de ce lien, incluant des œuvres protégées, sans que la personne ayant créé ledit lien en soit forcément consciente¹⁸¹.

Que faire ? La CJUE va faire mine d'ignorer que le public attiré par le lien est *objectivement* nouveau et va, en quelque sorte, inventer la notion de public « *subjectivement* nouveau ». Elle juge en effet :

[...] le fait de placer, sur un site Internet, des liens hypertexte vers des œuvres protégées, librement disponibles sur un autre site Internet sans l'autorisation du titulaire du droit d'auteur, constitue une « communication au public » au sens de cette disposition, il convient de déterminer si ces liens sont fournis sans but lucratif par une personne qui ne connaissait pas ou ne pouvait raisonnablement pas connaître le caractère illégal de la publication de ces œuvres sur cet autre site Internet ou si, au contraire, lesdits liens sont fournis dans un tel but, hypothèse dans laquelle cette connaissance doit être présumée¹⁸².

Lorsque l'œuvre est disponible sans restriction d'accès sur le site cible, il se forme donc une apparence, pour le candidat à la pose de lien, que son acte n'aura pas pour conséquence l'apparition d'un public nouveau - et tant pis s'il s'agit d'une réalité tout à fait extérieure à sa volonté. Cette apparence peut être dissipée par sa connaissance de l'illicéité, qui doit être prouvée. L'arrêt s'en serait-il tenu là, il y aurait déjà eu beaucoup à en dire. Mais afin de frapper plus facilement les sociétés qui battent monnaie de la diffusion illicite d'œuvres protégées, la connaissance du caractère illicite de la publication cible est présumée lorsque le poseur de lien agit « dans un but lucratif ». La notion est fuyante, bien plus que ne l'aurait été la référence à des critères proches de ceux qui fondent une profession : une répétition des actes dans le temps qui forme une habitude, et la

181. - §46.

182. - Extrait du dispositif de l'arrêt.

recherche de revenus substantiels. Le blogueur amateur qui a accepté d'insérer des publicités sur son site, et qui en tire quelques euros par mois, pourrait bien se retrouver entraîné dans une catégorie qui n'avait pas été pensée pour lui.

Il convient, pour finir cette étude de la jurisprudence récente de la CJUE, d'évoquer un arrêt de 2017 *Stichting Brein*¹⁸³. Il nous ramène à la question des réseaux de pair-à-pair, puisqu'il était question d'un site centralisant des liens BitTorrent, du nom de The Pirate Bay (TPB). Le protocole BitTorrent permet à des utilisateurs de réaliser des échanges décentralisés de fichiers, mais à la condition qu'ils amorcent l'opération en fournissant à leur logiciel — le « client BitTorrent » — un certain nombre de métadonnées. Le client sait ainsi ce qu'il doit rechercher et demander aux autres utilisateurs du réseau d'échange. Ces métadonnées sont recensées dans de grands annuaires, dont TPB n'est qu'un exemple. Ainsi, même si les liens dont il est question présentent une physionomie particulière — ils n'ouvrent pas une page Web, mais déclenchent un échange de données de pair-à-pair -, ils mènent vers des œuvres protégées diffusées sans autorisation. Les administrateurs de TPB en sont parfaitement conscients¹⁸⁴. Il n'est donc pas surprenant que la Cour y voie une forme de communication au public, certes un peu atypique par rapport aux arrêts précédemment cités. Toutefois, pour reprendre une formule de M. Cabrillac relative à une autre série jurisprudentielle complexe, « Reste à savoir si l'on peut se satisfaire de l'ajout d'une tourelle supplémentaire au château de Neuschwanstein au seul motif qu'elle respecte la symétrie générale »¹⁸⁵. En reculant de quelques pas, on aperçoit en effet un édifice d'une grande complexité. Les propositions doctrinales sont-elles d'un abord plus simple ?

218. Hyperliens et droit d'auteur : quelques suggestions doctrinales - Un récent rapport rédigé dans le cadre du Conseil supérieur de la propriété littéraire et artistique (CSPLA) formule des propositions en la matière¹⁸⁶. Les auteurs estiment que « [...] la jurisprudence est devenue aussi imprévisible que complexe et sinueuse »¹⁸⁷.

183. - CJUE, 14 juin 2017, *Stichting Brein c. Ziggo BV*, C-610/15.

184. - V. spéc. le 645 : « [...] il ressort des observations présentées à la Cour, d'une part, que les administrateurs de la plateforme de partage en ligne TPB ont été informés que cette plateforme, qu'ils mettent à la disposition des utilisateurs et qu'ils gèrent, donne accès à des œuvres publiées sans l'autorisation des titulaires de droits et, d'autre part, que les mêmes administrateurs manifestent expressément, sur les blogs et les forums disponibles sur ladite plateforme, leur objectif de mettre des œuvres protégées à la disposition des utilisateurs, et incitent ces derniers à réaliser des copies de ces œuvres ».

185. - R. Cabrillac, « Opposabilité d'une clause de non-garantie dans une chaîne homogène de contrats translatifs de propriété », *D.*, 2006, 971.

186. - P. Sirinelli, J.-A. Benazeraf et A. Bensamoun, *Mission droit de communication au public. Rapport et propositions*, Conseil supérieur de la propriété littéraire et artistique, décembre 2016 : www.culturecommunication.gouv.fr/Thematiques/Propriete-litteraire-et-artistique/Conseil-superieur-de-la-propriete-litteraire-et-artistique/Travaux/Missions/Mission-du-CSPLA-sur-le-droit-de-communication-au-public.

187. - *Ibid.*, p. 1.

L'une des voies explorées est la modification des textes, en l'occurrence de la directive 2001/29. Il s'agirait, d'abord, de définir très largement la communication au public comme « tout acte consistant à donner accès au public à une œuvre et/ou à un objet protégé »¹⁸⁸. Serait ensuite introduite une nouvelle exception « visant à soustraire certains hyperliens du droit de communication au public », sans plus recourir à la notion jurisprudentielle de « public nouveau ». Le poseur de lien serait ainsi « exemptés d'autorisation [...] » sous réserve :

i) que l'auteur de l'hyperlien ne sache pas ou n'ait pas de raisons valables de penser que le contenu pointé est communiqué au public ou mis à la disposition du public de manière illicite sur le service en-ligne vers lequel renvoie ce lien,

ii) et que cet œuvre et/ou objet protégé soit accessible sans restriction sur le service en-ligne vers lequel renvoie ce lien,

iii) et que la fourniture d'hyperlien n'ait pas été effectuée dans un but lucratif,

*iv) et que l'hyperlien ne permette pas d'afficher ou de diffuser directement l'œuvre ou l'objet protégé sur le service en-ligne à partir duquel il est établi*¹⁸⁹.

Si l'on s'attache aux effets concrets obtenus plutôt qu'aux techniques employées, la principale différence avec la jurisprudence de la CJUE semble résider dans le iv), qui traite distinctement les liens apparentés à la technique de la transclusion : ceux dont nous disions qu'ils réalisent une « découpe » au sein de la page source, permettant d'apercevoir l'œuvre liée directement, sans qu'il soit besoin de la quitter au profit d'une page cible¹⁹⁰. On se souviendra que certains juges de la Cour Suprême du Canada, interrogés sur le caractère potentiellement diffamatoire d'un lien hypertexte, souhaitent eux aussi traiter à part ceux qui représentent les propos cibles directement dans la page source¹⁹¹. Pour le surplus, tout en se débarrassant de l'insaisissable « public nouveau », la proposition aboutit à des résultats proches de ceux qui résultaient de la jurisprudence. Lorsqu'une page est librement accessible (iii), l'auteur du lien est libre de poser un lien sauf si le contenu visé n'était pas autorisé et qu'il est démontré qu'il le savait, ou aurait dû le savoir (i). La deuxième branche de l'alternative (les « raisons valables de penser » que le contenu est illicite) peut toutefois inquiéter, en raison de sa large indétermination. Si l'on se place dans la situation où le lien a déjà été posé, il semble sain de s'en remettre à l'appréciation du juge *in concreto*. Mais si l'on postule que les internautes connaissent la loi et cherchent à l'appliquer — voilà qui est audacieux —, ils vont

188. - *Ibid.*, p. 48 s.

189. - *Ibid.*, p. 53.

190. - Si l'on évoque les techniques « apparentées » à la transclusion, c'est parce que le rapport précise : « le texte proposé ne s'attache pas à la technique utilisée, mais à l'effet obtenu dans l'esprit de l'internaute utilisateur. Le but de cette rédaction est d'éviter que le texte proposé ne soit trop ancré dans une réalité technique susceptible d'être dépassée » (p. 55).

191. - V.supra, n°139.

quant à eux adopter une vision *a priori* : si je place ce lien, vais-je courir un risque juridique ? La plus grande prévisibilité est alors nécessaire ; il est à craindre qu'elle soit ici refusée. Enfin, le critère du « but lucratif » est à nouveau mobilisé. La CJUE l'utilisait indirectement, en tant qu'il entraînait une présomption de connaissance de l'illicéité éventuelle de la page cible. L'emploi est ici plus simple, plus direct, mais il continue à inquiéter, tant il est large. Les auteurs précisent en effet qu'« Il peut, par exemple, y avoir recherche d'un but lucratif dès lors que le site ou le service en ligne qui propose le lien perçoit des recettes publicitaires »¹⁹². Nous proposons plus haut l'exemple du simple particulier qui place une bannière de publicité sur son site et touche quelques euros par mois. On peut ajouter celui qui possède, sur le même site, des vidéos YouTube qui sont « monétisées » — ou le deviendront si elles rencontrent un succès populaire suffisant — ou même celui qui n'affiche aucune publicité, mais propose une boutique de « *goodies* », par exemple des t-shirts aux couleurs de son blog. C'est dire que le critère risque de frapper bien au-delà du cercle des professionnels sans scrupule de type GS Media ou TPB.

Pour toutes ces raisons, les propositions de Madame Bénabou, plus radicales, apparaissent aussi plus séduisantes¹⁹³. Elles font produire davantage d'effets à la distinction entre le lien « brut » et le lien apparenté aux techniques de transclusion.

*Le lien brut est un véhicule informationnel. Or, le lien qui pointe vers un contenu sans activer la perception de l'œuvre qu'on qualifiera de « lien brut » ne crée pas une communication au public de l'œuvre, faute précisément de « représenter » l'œuvre en elle-même. Il se contente de « motoriser » l'internaute vers sa destination ; c'est la métaphore du conducteur de taxi chère aux moteurs de recherche, plus encore que celle de la note de bas de page qui n'est qu'une information sur la situation de la source et non le véhicule pour s'y rendre. Le lien brut ne constitue pas un accès à l'œuvre, mais un moyen de parvenir à un tel accès. Il se situe en amont. Il n'existe pas d'effet substitutif : le poseur de lien ne retranche pas de parts de marché aux ayants droit puisque pour jouir de l'œuvre il faut toujours se rendre sur le site de destination*¹⁹⁴.

L'effet de simplification est spectaculaire. Quant aux usages atypiques de liens bruts, il est proposé de les traiter en invoquant d'autres corps de règles, afin de contourner le piège dans lequel s'est enfermée la CJUE, et que le rapport de la CSPLA ne semble pas esquiver totalement : celui de rendre la règle effrayante, car trop subtile, pour l'internaute ordinaire. Ainsi, lorsqu'un lien parvient à rendre accessible à tout public une œuvre qui était réservée, sur la page cible, à un public restreint, il est simplement proposé d'invoquer la violation des mesures techniques de protection, qui font

192. - P. Sirinelli, J.-A. Benazeraf et A. Bensamoun, rapport préc., p. 55. Les auteurs ajoutent : « La réutilisation de données personnelles recueillies par le service en-ligne qui propose l'hyperlien peut être regardée comme la poursuite d'un but lucratif ».

193. - Obs. précitées sur l'arrêt *GS Media*.

194. - *Ibid.*

l'objet de règles spécifiques - sur lesquelles nous reviendrons¹⁹⁵. Quant aux annuaires de liens illicites : « il n'est pas nécessaire de distordre le droit de communication pour parvenir à une solution satisfaisante : puisqu'il s'agit ici de lutter contre l'illicite, la voie pénale est alors à privilégier. Or, il n'est nullement nécessaire d'assimiler le lien à un acte de communication au public pour punir celui qui, intentionnellement, pointe vers des contenus illicites, il suffit de caractériser la complicité de contrefaçon par fourniture de moyens ou le recel »¹⁹⁶.

En revanche, l'auteur rejoint le rapport du CSPLA pour considérer qu'un lien de type « transclusion » réalise une représentation de l'œuvre, soumise à autorisation. La solution semble à la fois respectueuse de l'orthodoxie juridique et opportune : il n'est pas déraisonnable de demander à un internaute, lorsqu'il *intègre* une vidéo à sa propre page Web, de se poser la question de la licéité de son acte. Sur une plateforme comme YouTube, celui qui charge une vidéo sur la plateforme doit décider s'il active ou désactive la possibilité d'en réaliser une transclusion¹⁹⁷. Le fait que cette possibilité n'ait pas été désactivée devrait être interprété comme une autorisation donnée aux internautes de représenter la vidéo sur leur propre site - d'autant que les profits engendrés par la publicité qui accompagne la diffusion reste acquise à celui qui l'a versée sur le site. Il existerait donc des manières de régler le problème de l'autorisation du titulaire du droit lorsque la publication d'origine est licite. Reste à régler le cas, qui n'est pas rare, d'une publication originale non autorisée faisant l'objet d'une transclusion. Le titulaire du droit d'auteur aura d'abord à cœur d'agir auprès de la plateforme pour faire retirer le contenu, qui cessera aussitôt d'être disponible sur les sites l'ayant encapsulé. S'il souhaite néanmoins poursuivre les personnes ayant procédé à sa transclusion pour leur réclamer des dommages-intérêts, il serait opportun qu'il ait à démontrer que la personne connaissait l'illicéité. Quant à ceux qui sont spécifiquement organisés pour profiter, en toute connaissance de cause, de violations répétées du droit d'auteur, ils feront à nouveau l'objet d'un traitement pénal.

En attendant ces éventuelles réformes, et en dépit de la bonne volonté de la CJUE, on constate que le droit d'auteur résiste à la pratique spécifiquement numérique de la pose de liens hypertextes. À tout le moins, d'importantes frictions se produisent, qu'il serait bon d'éliminer sans tarder.

195. - V.infra, n° 230 s.

196. - V.-L. Benabou, obs. préc. sur l'arrêt *GS Media*.

197. - V. la page « Limiter l'intégration » de la plateforme : <https://support.google.com/YouTube/answer/6301625?hl=fr>.

b – La circulation transformative

219. **L'approche du droit américain** - Dans les situations précédemment évoquées, les technologies numériques étaient employées pour faire voyager une œuvre en laissant intacte sa forme : si des transformations purement techniques pouvaient lui être appliquées afin de faciliter sa circulation — des compressions, des changements de formats -, elles ne concernaient que le véhicule et non le contenu lui-même. Toute différente est la question de la circulation transformative : ici, une œuvre initiale sera revisitée, réinterprétée, déconstruite, altérée, entière ou par fragments. Sa communication à autrui n'est donc pas l'objectif principalement poursuivi : elle ne voyagera qu'incidemment, en tant qu'elle constitue un matériau de construction nécessaire à une œuvre nouvelle.

La question des usages transformatifs des œuvres protégées par le droit d'auteur est un thème récurrent dans l'œuvre de M. Lessig. Il a volontiers recours à des exemples, qui ne sont pas tous absolument du même ordre.

Dans son ouvrage de 2004 *Free culture*, il évoque les difficultés rencontrées par les auteurs d'un documentaire consacré à Clint Eastwood¹⁹⁸. Il devait être composé en partie d'entretiens accordés par l'acteur, mais les auteurs souhaitaient intégrer à leur création un grand nombre d'extraits de films. Une année entière fut nécessaire à leur équipe pour retrouver chacun des figurants aperçus dans les diverses scènes, chacun des compositeurs des musiques entendues durant quelques secondes. Il fallut ensuite négocier avec eux une contrepartie financière en échange du droit de ré-exploiter leur travail. L'ensemble du processus, selon les auteurs, est de nature à décourager la plupart des projets similaires¹⁹⁹.

Un peu plus loin, il évoque plus spécifiquement le numérique, et sa culture du « copier-coller », qui fournissent aux amateurs les moyens techniques d'exploiter la musique, les images, les vidéos préexistantes à des fins esthétiques, ludiques ou politiques²⁰⁰. En revanche, les moyens juridiques de

198. - L. Lessig, *Free culture*, op. cit., chap. 8 : *Transformers*, p. 100 et s.

199. - « *Everyone thought it would be too hard. Everyone just threw up their hands and said, "Oh, my gosh, a film, it's so many copyrights, there's the music, there's the screenplay, there's the director, there's the actors"* » (Alex Alben, cité par L. Lessig, op. cit., p. 102).

200. - *Ibid*, p. 105. « *We live in a "cut and paste" culture enabled by technology. Anyone building a presentation knows the extraordinary freedom that the cut and paste architecture of the Internet created—in a second you can find just about any image you want; in another second, you can have it planted in your presentation. But presentations are just a tiny beginning. Using the Internet and its archives, musicians are able to string together mixes of sound never before imagined; filmmakers are able to build movies out of clips on computers around the world. An extraordinary site in Sweden takes images of politicians and blends them with music to create biting political commentary. A site called Camp Chaos has produced some of the most biting criticism of the record industry that there is through the mixing of Flash! and music* ».

cette création leur seraient refusés : « *All of these creations are technically illegal. Even if the creators wanted to be “legal,” the cost of complying with the law is impossibly high. Therefore, for the law-abiding sorts, a wealth of creativity is never made* »²⁰¹.

Comme bien souvent au cours de cette étude, nous rencontrons une difficulté juridique qui a largement préexisté au numérique, mais qui prend à cause de lui — ou grâce à lui — une ampleur sans précédent.

Dans les exemples proposés par M. Lessig, plusieurs difficultés sont mises en évidence. La première tient à la complexité des procédures qui s'imposent aux auteurs d'œuvres dérivées : dans certaines situations, le plus coûteux, le plus difficile est d'identifier le titulaire du droit et d'entrer en contact avec lui. Lorsque c'est le cas, les amateurs sont déjà dissuadés. Ceux qui cherchent à produire une œuvre nouvelle à des fins lucratives procéderont peut-être à « l'investissement » nécessaire — en temps et en compétences -, mais cela aboutira à renchérir leurs coûts. S'ils ne peuvent se le permettre, c'en est terminé. Il est possible d'aplanir cette première difficulté en centralisant les informations sur les droits — dans des registres — voire en centralisant les droits eux-mêmes - c'est le rôle des sociétés collectives de gestion des droits d'auteur. Survient alors le deuxième problème : s'il faut recueillir l'autorisation des titulaires de droits, cela signifie qu'ils peuvent la refuser, et empêcher un usage transformatif de leur œuvre qui leur déplairait. Il ne s'agit pas, à ce stade, de se prononcer sur le bien ou mal-fondé du pouvoir qui leur est ainsi conféré, mais simplement de constater son existence. Enfin, si l'on suppose que le titulaire du droit est enclin à donner son autorisation, peut-être ne voudra-t-il pas le faire sans contrepartie monétaire, ce qui constitue une troisième difficulté. S'il faut payer un droit fixe trop élevé, les amateurs et les « petits professionnels » risquent à nouveau d'être évincés. Le danger sera moindre si c'est un système proportionnel qui est retenu : les profits faibles ou inexistantes donneront naissance à des dettes faibles ou inexistantes.

L'une des solutions proposées par M. Lessig a consisté en la mise au point de contrats types de licence, dits « licences libres », dont certains sont spécifiquement pensés pour permettre des usages transformatifs de l'œuvre, gratuits, avec ou sans caractère commercial selon les cas. Ils seront abordés plus loin²⁰². Ces outils ont vocation à simplifier considérablement les démarches des artistes transformatifs, en créant un véritable écosystème créatif autour de l'œuvre ainsi concédée. Mais ils requièrent que le titulaire du droit d'auteur sur l'œuvre d'origine s'inscrive volontairement, et par

201. - *Ibid.*, p. 106. Adde L. Lessig, « Laws that choke creativity », conférence TED mars 2007 : https://www.ted.com/talks/larry_lessig_says_the_law_is_strangling_creativity.

202. - V.infra, n° 240 s.

avance, dans une démarche de partage. Ce ne sera pas toujours le cas, et d'autres réponses doivent donc être recherchées.

En droit américain, une solution partielle réside dans le régime des exceptions au droit d'auteur. Contrairement au droit français, il existe dans les pays de *copyright* une exception « ouverte » appelée *fair use*²⁰³. La loi ne prévoit pas de cas à la fois précis et exhaustifs : elle se contente de poser des critères souples, dont le juge se saisira pour évaluer l'utilisation qui lui est déférée d'une œuvre sous *copyright*. Ces critères sont :

(1) *the purpose and character of the use, including whether such use is of a commercial nature or is for nonprofit educational purposes;*

(2) *the nature of the copyrighted work;*

(3) *the amount and substantiality of the portion used in relation to the copyrighted work as a whole; and*

(4) *the effect of the use upon the potential market for or value of the copyrighted work.*

*The fact that a work is unpublished shall not itself bar a finding of fair use if such finding is made upon consideration of all the above factors*²⁰⁴.

Lorsqu'un usage transformatif est qualifié par le juge de *fair use*, il est à la fois dispensé d'autorisation et de paiement d'une compensation financière. Mais jusqu'à ce qu'une éventuelle décision de justice intervienne, l'auteur de l'œuvre seconde n'a aucune assurance qu'il passera le *transformative test* ; or, s'il échoue, il s'expose à de lourdes sanctions²⁰⁵. Après avoir étudié l'ensemble de la jurisprudence pertinente de la Cour suprême et des Cours d'appel, un auteur résume ainsi les critères employés :

*[...] if you copy an original work, use it for a different purpose than the purpose for which the original work was created. Modify the contents, function and meaning of the original work through alteration of the original expression or the addition of significant new expression. Otherwise, you are making an unauthorized exploitation of the creative expression of the work for the exactly same reasons and purposes that the original author or artiste created the work, and you are depriving the original author or artiste of the derivative works right guaranteed by copyright*²⁰⁶.

203. - Sur cette différence, V. par ex. M. Vivant et J.-M. Bruguière, *op. cit.*, n° 602.

204. - 17 U.S. Code §107.

205. - Michael D. Murray, « What is Transformative? An Explanatory Synthesis of the Convergence of Transformation and Predominant Purpose in Copyright Fair Use Law », 11 *Chi. -Kent J. Intell. Prop.*, 260 (2012) : <http://scholarship.kentlaw.iit.edu/ckjip/vol11/iss2/8>

206. - *Ibid.*, p. 261. Pour un exemple de procès récent mettant en jeu l'application du *fair use* à une œuvre dérivée de Star Trek : C. Farivar, « Axanar isn't fair use, judge finds, setting stage for Star Trek copyright trial », article *arstechnica.com* du 1er mai 2017.

En droit français, la question se pose dans des termes différents, à la fois parce qu'il y existe un système fermé d'exceptions au droit d'auteur, mais surtout parce qu'un droit moral de l'auteur et de ses héritiers est susceptible d'être invoqué contre la possibilité de transformer une œuvre.

220. En France : le rapport de la mission du CSPLA - En 2013, une commission présidée par M. Pierre Lescure avait attiré l'attention des pouvoirs publics sur « le statut juridique excessivement précaire » des pratiques de création transformatrice²⁰⁷. L'année suivante, un rapport rédigé dans le cadre du CSPLA fut spécifiquement consacré à la question²⁰⁸.

L'ancienneté du phénomène de la « création seconde » est d'abord soulignée : La Fontaine revisite Ésope, Bacon retravaille Velazquez, Montaigne enrichit ses Essais de multiples fragments d'œuvres classiques. Certains artistes, comme Marcel Duchamp, abordent même frontalement la question : en affublant la Joconde d'un bouc, et d'une moustache, et en baptisant l'ensemble du titre provocateur L.H.O.O.Q., il fait de l'œuvre préexistante le centre de son propos²⁰⁹.

Les travaux de M. Aigrain sont ensuite évoqués, qui montrent que le numérique provoque à la fois un changement d'échelle, mais aussi et plus fondamentalement un bouleversement social.

Quelle est la grande transformation qu'a apporté le numérique (entendu comme combinaison de l'informatique, d'Internet et du Web) dans le champ culturel ? C'est avant tout une immense capacitation culturelle, une capacité accrue à créer et s'exprimer :

- *multiplication par 100 du nombre de personnes qui ont accès à la publication et la distribution de contenus à destination ouverte,*
- *division par 10 à 100 du coût de production de contenus selon les médias,*
- *apprentissage simplifié des fonctions techniques de création.*

Les compétences expressives restent bien sûr plus difficiles à s'approprier, mais les processus sociaux liés la création sur Internet et à ses retombées dans l'espace social physique permettent à chacun de progresser. On pourrait donc considérer que la naissance et la diffusion sociale du numérique à elle seule va enrichir considérablement la culture au sens large²¹⁰.

207. - P. Lescure (dir.), *Contribution aux politiques culturelles à l'ère numérique*, t. 1, 2013, p. 36.

208. - V.-L. Bénabou (présidente) et F. Langrognet (rapporteur), *Rapport de la mission du CSPLA sur les « œuvres transformatrices »*, 2014, disponible sur www.culturecommunication.gouv.fr. Voir aussi la thèse de P. Léger, *La recherche d'un statut de l'œuvre transformatrice. Contribution à l'étude de l'œuvre composite en droit d'auteur*, dir P. Sirinelli, 2015.

209. - *Ibid.*, p. 3.

210. - P. Aigrain, « Culture et partage : les conditions d'existence des communs culturels », blog paingrain.debatpublic.net, article du 9 décembre 2012. L'auteur aborde cependant ensuite les obstacles, y compris juridiques, au développement de ces potentialités.

En abordant la liberté de communication, nous avons décrit un mouvement du même ordre. D'une catégorie spécialisée et étroite de la population — les journalistes, les artistes — qui diffuse sa production vers ses semblables, le numérique permettrait d'évoluer vers un modèle dans lequel chacun contribue aussi bien qu'il consomme²¹¹. Ce modèle ne remplace pas le précédent, mais s'y ajoute : il est bon qu'existent des professionnels de ces activités, placés dans les meilleures conditions matérielles et de formation pour exercer au plus haut niveau. Mais il est réjouissant que chacun puisse s'essayer à l'expression publique, y compris l'expression artistique. Or, la possibilité de réinterpréter l'existant plutôt que de partir — en apparence — de rien est de nature à encourager de telles démarches.

Le rapport présente ensuite quelques exemples marquants de pratiques transformatives contemporaines, parmi lesquels, les *mashups* et *remix*, qui font entrer en collision des fragments audio ou vidéos tirés d'œuvres existantes pour leur donner un sens nouveau, ou encore les *fanvids*, qui rassemblent diverses séquences d'une œuvre de cinéma ou de télévision, en les assortissant d'un montage très dynamique et d'une musique nouvelle²¹². Les *fan-fictions*, quant à elles, sont des histoires écrites par des amateurs, sur la toile de fond fournie par une œuvre littéraire ou audiovisuelle à succès : elles prolongent le récit officiel, le précédent, proposent des versions alternatives d'un événement marquant ou d'une relation entre personnages. La mission souligne le rôle joué par la saga Harry Potter dans le développement de cette forme d'expression : elle aurait donné lieu à l'écriture de plus de 35 000 histoires par les fans²¹³. On aurait pu aisément rajouter à cette liste les *mods*, qui constituent des variations sur un jeu vidéo d'origine, développées par des tiers, souvent des amateurs offrant leur travail à la communauté des joueurs²¹⁴.

Le groupe de travail s'interroge ensuite sur la terminologie à employer, mais aussi, ce faisant, sur le fond des concepts et sur les limites de la mission qui lui a été confiée. Les expressions « œuvre transformative, création transformative et usage transformatif » ne sont vraiment connues ni des artistes, ni des juristes francophones : il s'agit d'une traduction du *transformative test* dans le cadre du *fair use* de droit américain²¹⁵. L'expression *user-generated content (UGC)*, « contenus créés par

211. - V.supra, n°123. Dans le même sens : L. Lessig, *Free culture*, op. cit., p. 37 : « *Couch potatoes. Consumers. This is the world of media from the twentieth century. The twenty-first century could be different. This is the crucial point: It could be both read and write. Or at least reading and better understanding the craft of writing. Or best, reading and understanding the tools that enable the writing to lead or mislead* »

212. - V.-L. Bénabou (présidente) et F. Langrognet (rapporteur), *Rapport de la mission du CSPLA sur les « œuvres transformatives »*, préc., p. 9 s.

213. - *Ibid.*, p. 11.

214. - Sur cette pratique, V. par ex. L. Maurel, « Valve et le casse-tête de la monétisation des usages transformatifs », article *scinfolex.com* du 15 mai 2015.

215. - *Ibid.*, p. 13.

les utilisateurs », est mieux connue à défaut d'être plus précise. Elle renvoie à une situation dans laquelle un outil ou une plateforme fédère une communauté qui sécrète des biens culturels : les contributeurs de Wikipédia écrivent des articles, les utilisateurs de YouTube y versent des vidéos, ceux de Flickr y placent des photos, les joueurs du jeu vidéo Second Life peuplent l'univers d'objets qu'ils ont conçus. La catégorie est donc particulièrement hétérogène. Les UGC peuvent ne pas correspondre à des œuvres protégées par le droit d'auteur - une vidéo YouTube qui ne serait qu'une réplique d'un contenu antérieur, ou une photo Flickr dépourvue de toute originalité dans son sujet et son cadrage. Elles peuvent consister en une création « première » : un article Wikipédia ou une photo portant l'empreinte de la personnalité de son auteur en constituent des exemples. Elles sont aussi, il est vrai, des vecteurs courants d'œuvres secondes : les mashups et fanvids prolifèrent sur YouTube et Dailymotion ; les fanfictions sont centralisées sur des plateformes.

La mission considère donc, à juste titre, qu'elle doit abandonner la référence aux UGC et consacrer ses travaux à la création transformative, aussi nouveaux que soient ces termes. Elle s'interroge alors sur sa conformité au droit positif.

221. En droit positif : des exceptions insuffisantes - Pour qu'un problème se pose, encore faut-il qu'une œuvre seconde se heurte à la protection accordée par le droit d'auteur à une œuvre première. Tel n'est pas le cas, rappelle la mission, lorsque sont repris de minuscules fragments de l'œuvre initiale, non représentatifs de sa forme globale²¹⁶. Ce n'est pas le cas non plus lorsque la reprise de l'œuvre première dans l'œuvre seconde est indirecte, incidente, « fortuite », telles ces couvertures de manuels illustrées que l'on aperçoit au détour du documentaire *Être et avoir* comme de simples éléments du décor, « non représentés pour eux-mêmes »²¹⁷.

216. - CJUE, *Infopaq International A/S c./ Danske Dagblades Forening*, 16 juillet 2009, C-5/08, §45 : « S'agissant des éléments de telles œuvres sur lesquels porte la protection, il convient de relever que celles-ci sont composées de mots qui, considérés isolément, ne sont pas en tant que tels une création intellectuelle de l'auteur qui les utilise. Ce n'est qu'à travers le choix, la disposition et la combinaison de ces mots qu'il est permis à l'auteur d'exprimer son esprit créateur de manière originale et d'aboutir à un résultat constituant une création intellectuelle ».

217. - Cass. 1ère civ., 12 mai 2011, n° 08-20.651 : « [...] attendu que l'arrêt relève que, telles que figurant dans le film documentaire en cause et dans le bonus des DVD, les illustrations dont M. X... est l'auteur ne sont que balayées par la caméra et vues de manière fugitive, que plus fréquemment elles sont à l'arrière-plan, les personnages des élèves et du maître étant seuls mis en valeur, qu'elles ne sont à aucun moment présentées dans leur utilisation par le maître et font corps au décor dont elles constituent un élément habituel, apparaissant par brèves séquences, mais n'étant jamais représentées pour elles-mêmes ; que la cour d'appel en a exactement déduit qu'une telle présentation de l'œuvre litigieuse était accessoire au sujet traité résidant dans la représentation documentaire de la vie et des relations entre maître et enfants d'une classe unique de campagne, de sorte qu'elle devait être regardée comme l'inclusion fortuite d'une œuvre, constitutive d'une limitation au monopole d'auteur, au sens de la Directive 2001/29/CE du 22 mai 2001, telle que le législateur a, selon les travaux préparatoires, entendu la transposer en considération du droit positif [...] ». V. déjà, en ce sens, l'affaire *Place des terreaux* présentée par le rapport, p. 30.

Si l'œuvre est originale et suffisamment présente au sein de l'œuvre seconde, elle est susceptible d'être reproduite ou représentée avec elle, ce qui a pour effet d'activer les droits patrimoniaux de l'auteur - la question du droit moral sera abordée plus loin. Il faut alors recueillir son autorisation, et lui verser une rémunération, sauf à ce qu'il ait consenti par avance une « licence libre » autorisant les usages dérivés, ou qu'il soit possible d'invoquer une exception au droit d'auteur. Le rapport examine très rigoureusement la possibilité d'exploiter les exceptions existantes au profit de la création transformative. Les grandes lignes de cet examen doivent être rappelées. Il y est procédé « selon un crescendo de la prise en compte de la “transformativité” »²¹⁸.

L'exception pédagogique est abordée en premier lieu²¹⁹. Elle pourrait avoir un intérêt dans le cadre d'usages transformatifs bien précis, par exemple l'utilisation d'œuvres à l'appui d'un support de cours d'histoire de l'art. Mais la mission souligne le manque d'ambition du texte, qui limite l'utilisation à des « extraits » et non à des œuvres complètes²²⁰. Aussi et surtout, l'exigence d'un public « majoritairement » composé d'étudiants, d'enseignants et de chercheurs condamne toute publication de l'œuvre seconde sur un site accessible à tous, et la cantonne de fait aux Espaces numériques de travail (ENT) des établissements d'enseignement²²¹.

L'exception de citation est plus intéressante. L'auteur ne peut en effet interdire « Les analyses et courtes citations justifiées par le caractère critique, polémique, pédagogique, scientifique ou d'information de l'œuvre à laquelle elles sont incorporées »²²². Comme l'écrivent les auteurs du rapport, « A priori, l'exception de citation constitue la terre d'élection de la création transformative, véritable permission légale de reprendre une œuvre antérieure pour l'incorporer dans une œuvre seconde »²²³. Le fait que la citation doive être « courte » constitue toutefois une première contrainte.

218. - V.-L. Bénabou (présidente) et F. Langrogné (rapporteur), *Rapport de la mission du CSPLA sur les « œuvres transformatives »*, préc., p. 50.

219. - En vertu de l'art. L. 122-5 CPI, 3, e, l'auteur ne peut interdire « La représentation ou la reproduction d'extraits d'œuvres, sous réserve des œuvres conçues à des fins pédagogiques et des partitions de musique, à des fins exclusives d'illustration dans le cadre de l'enseignement et de la recherche, y compris pour l'élaboration et la diffusion de sujets d'examens ou de concours organisés dans la prolongation des enseignements à l'exclusion de toute activité ludique ou récréative, dès lors que cette représentation ou cette reproduction est destinée, notamment au moyen d'un espace numérique de travail, à un public composé majoritairement d'élèves, d'étudiants, d'enseignants ou de chercheurs directement concernés par l'acte d'enseignement, de formation ou l'activité de recherche nécessitant cette représentation ou cette reproduction, qu'elle ne fait l'objet d'aucune publication ou diffusion à un tiers au public ainsi constitué, que l'utilisation de cette représentation ou cette reproduction ne donne lieu à aucune exploitation commerciale et qu'elle est compensée par une rémunération négociée sur une base forfaitaire [...] ».

220. - Rapport précité, p. 51.

221. - *Ibid.*, p. 12.

222. - Art. L. 122-5 CPI, 3, a).

223. - Rapport précité, p. 52.

Mais l'obstacle le plus important est ailleurs : la jurisprudence française considère que seul un texte peut, à proprement parler, faire l'objet d'une « citation », ce qui exclut par exemple toute utilisation d'un fragment sonore, d'une partie d'image ou d'un morceau d'œuvre plastique²²⁴. Voici qui appauvrit considérablement l'intérêt de l'exception dans la perspective de la création transformative. Pourtant, là où le texte ne distingue pas, il ne devrait pas y avoir lieu de distinguer. Les auteurs du rapport voudraient voir dans un arrêt *Eva-Maria Painer* de la CJUE la preuve que cette juridiction retient, quant à elle, une conception plus ouverte des œuvres susceptibles d'être citées²²⁵. Ce serait heureux. Hélas, il nous semble que la Cour évite au contraire soigneusement de se prononcer sur cette question²²⁶. En revanche, cet arrêt reconnaît que la citation peut intervenir dans le cadre d'un usage qui ne répond pas lui-même nécessairement à la qualification d'œuvre nouvelle – par exemple parce qu'il n'est pas suffisamment original²²⁷. Mais ainsi restreinte au seul usage de texte, l'exception de courte citation se révèle particulièrement décevante pour qui souhaiterait la promotion des œuvres transformatives. Quand bien même elle évoluerait à l'avenir de ce point de vue, il faudrait encore garder à l'esprit que toute citation courte n'est pas licite : une liste limitative de finalités poursuivies est imposée, qui sont « explicatives ou informationnelles plutôt que créatives »²²⁸ et encore moins récréatives.

L'exception de parodie est examinée pour finir²²⁹. La notion a été définie par la CJUE : « [...] la parodie a pour caractéristiques essentielles, d'une part, d'évoquer une œuvre existante, tout en

224. - M. Vivant et J.-M. Bruguière, *op. cit.*, n° 642, qui regrettent cette position et soulignent la dissidence de CA Paris, 4e ch., 12 oct. 2007 : « rien ne permet d'exclure les œuvres photographiques du champ d'application de l'article L. 122-5 3° ».

225. - V.-L. Bénabou (présidente) et F. Langrognet (rapporteur), *Rapport de la mission du CSPLA sur les « œuvres transformatives »*, préc., p. 53 : « Cette lecture “restrictive” de l'exception de citation a récemment fait l'objet d'un assouplissement par la jurisprudence européenne de la CJUE dans l'affaire *Eva Maria Painer*. Repoussant l'argument de l'impossibilité de citer une œuvre graphique, la Cour a considéré que la citation d'une photographie est tout à fait envisageable ».

226. - CJUE, 1er décembre 2011, *Eva-Maria Painer c./ Standard VerlagsGmbH* C-145/10, § 121 et s. : « [...] il est constant que l'œuvre évoquée dans l'affaire au principal est une photographie de portrait de Natascha K. Or, il convient d'observer que la juridiction de renvoi part de l'hypothèse selon laquelle une œuvre photographique relève du champ d'application de l'article 5, paragraphe 3, sous d), de la directive 2001/29. Par ailleurs, une telle hypothèse n'est contestée par aucune des parties au principal, par aucun des États membres ayant déposé des observations, ni par la Commission européenne. C'est dans cette perspective, **sans se prononcer sur le bien-fondé de ladite hypothèse** ni sur la question de savoir si les photographies litigieuses ont été effectivement utilisées dans le but de citation, qu'il convient de répondre à la deuxième question, sous a) et b) » (souligné par nous). Dans le même sens, V. les obs. de F. Pollaud-Dulian sur cet arrêt : *RTD. com.*, 2012, p. 120.

227. - § 137 : « (...) le fait qu'un article de presse citant une œuvre ou un autre objet protégé n'est pas une œuvre littéraire protégée par le droit d'auteur ne fait pas obstacle à l'application de [l'article 5, paragraphe 3, sous d), de la directive 2001/29] ».

228. - Rapport précité, p. 53.

229. - L'auteur ne peut en effet interdire : « La parodie, le pastiche et la caricature, compte tenu des lois du genre » : art. L. 122-5 CPI, 4).

présentant des différences perceptibles par rapport à celle-ci, et, d'autre part, de constituer une manifestation d'humour ou une raillerie »²³⁰. La déception éprouvée à l'analyse des précédentes exceptions n'est donc pas de mise ici : la parodie se révèle particulièrement accueillante. En particulier, l'humour absurde et outrancier propre à Internet trouve ici une terre d'asile, ce qu'on appelle le même : un objet culturel quelconque — une phrase, une image, une vidéo, une situation — qui fait l'objet de milliers d'interprétations en quelques heures, jusqu'à la nausée²³¹. Cette œuvre primaire, détournée des centaines de fois, est parfois elle-même transformative — ainsi d'une vidéo mettant en scène l'étonnante promenade d'une photographie de l'acteur Adrien Brody au sein de paysages variés²³² —, parfois non — la célèbre photo de « l'homme à la pelle », illustrant un article de presse²³³.

222. Les recommandations de la mission à droit constant - Celles-ci s'articulent en deux séries : la première basée sur un scénario à droit constant, la seconde sur une évolution du droit.

En l'absence d'intervention législative, la mission estime que l'obstacle majeur réside dans « (...) la complexité du droit et l'existence de coûts de transaction hors de proportion avec l'intérêt de la réalisation de l'opération [...] »²³⁴. En cela, elle rejoint parfaitement le constat dressé par Lawrence Lessig²³⁵. Les propositions consistent notamment à mieux informer les individus sur les règles applicables, sur les œuvres relevant du domaine public — légal ou « consenti » par certaines licences libres -, permettre une identification simple et rapide des œuvres existantes²³⁶. Vient ensuite une idée plus inattendue. Les auteurs mentionnent une pratique courante de la part des plateformes de partages de contenus : lorsqu'elles identifient, par des procédés automatisés, l'utilisation d'une œuvre protégée par le droit d'auteur, elles ne procèdent pas nécessairement à son retrait. Elles proposent souvent au titulaire du droit de le « monétiser » - c'est-à-dire d'en tirer des revenus, généralement publicitaires. S'inspirant de ces pratiques, la mission propose :

[...] (d')insérer dans les conditions générales d'utilisation (CGU) des plateformes d'hébergement une clause accordant à ces dernières un mandat pour représenter leurs

230. - CJUE, 3 septembre 2014, *Johan Debeckmyn c./ Helena Vandersteen*, C-201/13, § 20.

231. - D. Leloup, « Le même, ou l'art du détournement historique sur Internet », article *lemonde.fr* du 1er mai 2012 : « un objet culturel, le plus souvent humoristique, qui se diffuse très vite au sein d'une communauté en ligne, chacun des membres de cette communauté pouvant se réapproprier l'objet et en créer sa propre version ».

232. - Lemon Demon, « Brodyquest » : <https://www.YouTube.com/watch?v=ygI-2F8ApUM>.

233. - J. Toussay, « Pour la première fois, "l'homme à la pelle" témoigne... », article *huffingtonpost.fr* du 9 février 2017.

234. - V.-L. Bénabou (présidente) et F. Langrognet (rapporteur), *Rapport de la mission du CSPLA sur les « œuvres transformatives »*, préc., p. 68.

235. - V.supra, n°219.

236. - Rapport préc., p. 68 s.

clients auprès des ayants droit, aux fins d'obtenir l'autorisation d'exploitation nécessaire [...]. Ainsi la plateforme négocierait l'accès au répertoire au nom de l'ensemble des exploitations réalisées par ses clients dans le cadre d'un mécanisme global. Un tel dispositif aurait pour effet vertueux de liciter les actes réalisés par les utilisateurs, sans que ces derniers aient à s'acquitter personnellement de la demande d'autorisation et à en discuter les conditions individuellement. La plateforme négocierait un accord de représentation générale pour le compte de l'ensemble des personnes l'ayant mandatée. Ce mécanisme de rémunération « forfaitaire » pourrait prendre en considération les bénéfices d'exploitation issus de la diffusion des œuvres du répertoire, mais aussi le pourcentage d'œuvres dont la reprise est couverte par le bénéfice d'une exception gratuite (citation, parodie, etc.). Le système de rémunération pourrait également ouvrir droit à un traitement différencié des contenus en fonction d'indicateurs d'audience offerts par les plateformes²³⁷.

La proposition est séduisante. Cependant, elle appelle au moins deux réserves, dont les auteurs du rapport sont conscients. La première : si une grande partie des œuvres transformatives transite par des plateformes, ce n'est pas le cas de toutes. La seconde : « [...] ces pratiques contractuelles reposent sur la bonne volonté des opérateurs. Si une plateforme refuse d'introduire ce mécanisme de mandat, rien ne l'y contraint [...] »²³⁸.

223. Les pistes de réforme de la mission - Il est donc opportun d'envisager la voie d'une intervention législative. Plusieurs pistes sont passées en revue successivement. Toutes ne seront pas reprises ici.

Puisqu'elles participent à la diffusion des pratiques transformatives, la question d'un meilleur encadrement légal des « licences libres » est évoquée : nous envisagerons ces contrats plus loin²³⁹.

Le rapport se fait ensuite très prudemment l'écho d'une proposition de la Quadrature du Net, qui vise à reconnaître dans le chef des internautes un droit au partage d'œuvres numériques, en ce compris les œuvres transformatives, aux deux conditions qu'il s'agisse d'un partage décentralisé — transitant par des réseaux de pair-à-pair — et non marchand²⁴⁰. Sans rien enlever au mérite de cette proposition, on doit relever qu'elle se heurterait à de fortes résistances.

237. - *Ibid.*, p. 72.

238. - *Ibid.*, p. 73.

239. - V.infra, n° 240 s.

240. - La Quadrature du Net, *Eléments pour la réforme du droit d'auteur et des politiques culturelles liées*, non daté, proposition n°1 : <https://www.laquadrature.net/fr/elements-pour-la-reforme-du-droit-dauteur-et-des-politiques-culturelles-liees#partagenonmarchand> ; P. Aigrain, « Comment délimiter le partage non-marchand entre individus ? », article *paigrain.debatpublic.net* du 13 février 2012.

Suit un rejet attendu d'une transposition pure et simple du *fair use* en droit français. Extirper un mécanisme de son milieu d'origine pour le transplanter dans une culture juridique radicalement différente est toujours une opération vouée à l'échec²⁴¹.

La piste consistant en un élargissement du champ de l'exception de citation semble ainsi plus sérieuse. Précisons qu'une réforme nous semble nécessaire pour lui conférer un caractère « transmédia », puisque nous estimons que la jurisprudence *Eva-Maria Painer* ne l'a pas consacré²⁴². Le rapport aborde surtout l'hypothèse d'un élargissement des finalités admissibles pour la citation, avec la prise en compte des finalités créatives. L'idée est toutefois considérée avec circonspection : la convention de Berne impose qu'une exception au droit d'auteur soit spéciale, qu'elle ne porte pas atteinte à l'exploitation normale de l'œuvre et qu'elle ne cause pas de préjudice injustifié aux intérêts légitimes de l'auteur (c'est l'exigence dite « du triple test »)²⁴³. D'après le rapport, une exception de citation trop largement comprise pourrait à la fois manquer à la condition de spécialité, et porter atteinte aux intérêts légitimes de l'auteur. Après l'avoir élargie, il faudrait donc la resserrer, par exemple en distinguant les simples « usages » transformatifs des véritables « œuvres » transformatives, ou en se cantonnant aux citations « non commerciales ». Or, la mise au point de ces distinctions, en particulier la seconde, semble extrêmement difficile aux auteurs. La conclusion sur ce point est la suivante : « L'intégration d'une finalité créative ou transformative dans l'exception de citation rompt l'équilibre du mécanisme fondé sur la dimension essentiellement informationnelle de l'œuvre dans le cadre de la citation »²⁴⁴.

La proposition la plus forte se révèle alors être une version remaniée du mandat conféré aux plateformes de diffusion, musclée par la possibilité d'un recours à la loi. L'objectif serait de

(...) Parvenir à mettre en place un mécanisme de centralisation des autorisations lorsque la diffusion est opérée par l'intermédiaire d'une plateforme, soit par l'imputation directe d'un acte d'exploitation dans le chef de la plateforme au terme d'une réinterprétation des régimes de responsabilité, soit par des mécanismes de mandat (contractuel ou légal) d'obtention des autorisations nécessaires confiés par

241. - V.-L. Bénabou (présidente) et F. Langrognet (rapporteur), *Rapport de la mission du CSPLA sur les « œuvres transformatives »*, préc., p. 80.

242. - Sur cette question, V. aussi L. Maurel, « Pourquoi nous avons besoin d'un droit de citation audiovisuelle », article *scinfolex.com* du 17 octobre 2015 ; J. Reda (du « parti pirate »), *Rapport sur la mise en œuvre de la directive 2001/29/CE du Parlement européen et du Conseil du 22 mai 2001 sur l'harmonisation de certains aspects du droit d'auteur et des droits voisins dans la société de l'information*, 24 juin 2015 (2014/2256 (INI)).

243. - Convention de Berne pour la protection des œuvres littéraires et artistiques, 9 septembre 1886 (réd. 28 septembre 1979), article 9, 2°.

244. - V.-L. Bénabou (présidente) et F. Langrognet (rapporteur), *Rapport de la mission du CSPLA sur les « œuvres transformatives »*, préc., p. 85.

*leurs clients aux plateformes*²⁴⁵.

224. Les projets européens – La proposition de directive sur le droit d’auteur dans le marché numérique, révélée fin 2016 par la Commission européenne, ne formule aucune proposition spécifique s’agissant des usages transformatifs²⁴⁶.

En revanche, un rapport rendu sur ce projet de texte par la Commission de la culture et de l’éducation tente de se saisir de la question²⁴⁷. Un amendement est proposé, qui serait ainsi libellé :

Article 5 ter - Exception relative aux contenus générés par les utilisateurs

Les États membres prévoient une exception ou une limitation aux droits visés aux articles 2 et 3 de la directive 2001/29/CE, à l’article 5, point a), et à l’article 7, paragraphe 1, de la directive 96/9/CE, à l’article 4, paragraphe 1, point a), de la directive 2009/24/CE et à l’article 13 de la présente directive pour permettre l’utilisation numérique de citations ou d’extraits d’œuvres et d’autres objets protégés figurant dans des contenus générés par les utilisateurs à des fins de critique, de commentaire, de divertissement, d’illustration, de caricature, de parodie ou de pastiche à condition que ces citations ou extraits:

a) concernent des œuvres ou autres objets protégés ayant déjà été licitement mis à la disposition du public;

b) s’accompagnent d’une indication de la source, notamment le nom de l’auteur, sauf si cela s’avère impossible; et

*c) soient conformes aux bons usages et utilisés dans la mesure justifiée par le but poursuivi. Toute disposition contractuelle contraire à l’exception prévue au présent article est sans effet*²⁴⁸.

Il s’agit finalement d’élargir l’exception de citation d’une manière très proche de celle repoussée par la CSPLA. Les craintes relatives au respect du test en trois étapes sont ici avivées par le recours à des notions molles comme celles de « contenus générés par les utilisateurs » ou encore de « bons usages ». En dessous de la proposition, il est certes précisé : « Une telle exception ne peut s’appliquer qu’en vertu du “test en trois étapes”, protégeant ainsi les titulaires de droits contre des utilisations disproportionnées », mais, à ce stade, il s’agit d’un vœu pieux²⁴⁹.

245. - *Ibid.*, p. 92.

246. - Proposition de directive du Parlement européen et du Conseil sur le droit d’auteur dans le marché unique numérique, 14 septembre 2016, 2016/0280 (COD).

247. - M. Joulaud (rapp.), *Projet d’avis de la commission de la culture et de l’éducation sur la proposition de directive du Parlement européen et du Conseil sur le droit d’auteur dans le marché unique numérique*, 6 février 2017, 2016/0280 (COD).

248. - P. 47 du rapport précité.

249. - Extrait de la justification figurant sous la proposition d’amendement. Pour une appréciation optimiste de cette proposition : L. Maurel, « Enfin un “upgrade” de l’exception de citation dans la prochaine directive sur le droit d’auteur ? », article *scinfolex.com* du 14 février 2017.

225. **Une licence légale pour les usages transformatifs ?** - Au cours de ses réflexions sur les usages transformatifs, Lawrence Lessig évoque l'idée d'une licence légale (*statutory license*)²⁵⁰. Plutôt que de créer une exception au droit d'auteur, on peut en effet imaginer que la loi donnerait elle-même la permission d'utiliser une œuvre protégée, déjà diffusée, à des fins transformatives, en échange d'un droit proportionnel aux recettes. Elle aurait un rôle subsidiaire : si l'usage — qu'il mérite ou le qualificatif d'œuvre nouvelle — bénéficie d'une exception ou d'une licence libre, il ne serait pas nécessaire d'y recourir. Dans le cas contraire, le bénéfice de la licence légale pourrait être revendiqué par l'utilisateur, et enregistré dans un registre²⁵¹. La règle ne distinguerait pas, dans son principe même, selon qu'un but lucratif est poursuivi ou non, mais l'internaute ne tirant aucun profit de sa création n'aurait logiquement rien à verser.

Il faudra certes déterminer ce que sont des revenus pris en compte au titre des recettes – on pourrait tenir compte, par exemple, des recettes publicitaires générées par l'exploitation de l'usage transformatif sur un site personnel. Des contrôles devront également être diligentés, mais tel est déjà le cas lorsqu'une cession de droits est consentie volontairement par l'auteur : la rémunération proportionnelle est de principe, selon la loi²⁵². Le taux de la redevance pourrait être relativement élevé, ou proportionnel, ce qui encouragerait ceux qui comptent tirer des bénéfices de l'usage transformatif à conclure un accord avec le titulaire du droit d'auteur lorsque cela est possible.

Dans la lignée des propositions du rapport de la CSPLA, cette licence légale devrait intégrer les plateformes dans sa conception. Aussi préciserait-elle que les droits proportionnels doivent être payés par l'éventuel diffuseur sur les bénéfices qu'il tire lui-même de l'opération. Il pourrait donc y avoir deux contributeurs, si celui qui réalise l'usage transformatif en tire des bénéfices, ou n'y en avoir qu'un, si la plateforme est seule à produire des gains.

Deux tempéraments à ces règles imaginaires doivent être apportés. D'abord, que l'on se situe dans un paradigme d'exception au droit d'auteur ou de licence légale, la dérogation apportée au monopole de l'auteur n'est acceptable que si l'usage est réellement transformatif. Une diffusion pure et simple de l'œuvre première déguisée en transformation ne doit bénéficier d'aucune faveur.

250. - L. Lessig, *Free culture*, op. cit., p. 103 : « *Would it make sense, I asked, for there to be some kind of statutory license that someone could pay and be free to make derivative use of clips like this? Did it really make sense that a follow-on creator would have to track down every artist, actor, director, musician, and get explicit permission from each? Wouldn't a lot more be created if the legal part of the creative process could be made to be more clean?* ».

251. - On pourrait également imaginer que la licence s'applique de plein droit, mais il faudrait alors des moyens importants pour assurer le suivi des usages dérivés sans la collaboration des utilisateurs.

252. - Art. L. 131-4 CPI : « La cession par l'auteur de ses droits sur son œuvre peut être totale ou partielle. Elle doit comporter au profit de l'auteur **la participation proportionnelle aux recettes** provenant de la vente ou de l'exploitation » (souligné par nous). La suite du texte prévoit, par exception, des situations de rémunération forfaitaire.

Cela crée certes une incertitude, mais elle est indépassable et relève du concept même d'usage transformatif, qui traînera toujours dans son sillage une forme de parasitisme contre laquelle il faudra bien lutter. Ensuite, le droit moral de l'auteur doit pouvoir être invoqué pour s'opposer aux usages qui trahissent profondément l'œuvre initiale. Quelques précisions doivent être apportées à ce propos.

226. La signification du droit moral de l'auteur – Dans son rapport, la mission de la CSPLA apporte une très importante précision :

Il est apparu lors des auditions que nombre des personnes consultées avaient une représentation erronée du droit moral, notamment pour en surestimer l'effet de blocage vis-à-vis de la transformation. Il est, à notre sens, important de souligner que le droit moral constitue une défense de l'auteur contre une atteinte à certaines prérogatives que la loi a entendu consacrer à son bénéfice et non un droit requérant systématiquement de celui qui utilise l'œuvre une autorisation préalable²⁵³.

Les pays de copyright ne connaissent pas d'équivalent du droit moral. Dans la tradition française, ce fil d'or qui relie pour toujours l'œuvre au créateur, puis à ses héritiers, est considéré avec une grande révérence²⁵⁴. Il doit cependant être considéré avec prudence : les héritiers de Léonard de Vinci devraient-ils pouvoir interdire *L.H.O.O.Q.*, sous prétexte que Duchamp trahit l'esprit originel de l'œuvre²⁵⁵ ? Le CSPLA rappelle à juste titre quels sont les attributs du droit moral : un droit de divulgation, qui s'épuise lorsque l'œuvre est révélée au monde ; un droit à la paternité, qui doit être respecté en toute hypothèse, en matière d'usage transformatif autant qu'ailleurs ; un droit au respect de l'intégrité de l'œuvre. Ce dernier est ici le plus important. Sa portée ne doit pas être surestimée : les héritiers d'Hugo estimaient que, par principe, « le caractère achevé » de l'œuvre ainsi que son éminent mérite interdisaient qu'on donne une suite aux *Misérables*. La Cour de cassation a répondu que ces motifs étaient inopérants, et qu'il faudrait, pour qu'il y ait atteinte au droit moral, exposer en quoi l'œuvre avait été « altérée »²⁵⁶. Le mot est bien choisi : l'œuvre d'origine doit avoir été abîmée par la transformation. Cela se produit parfois : un dessinateur a récemment mis en scène la mort du personnage de grenouille qu'il avait créé, et qui était devenu, à son désespoir, un symbole de ralliement de l'extrême droite²⁵⁷. Les abus doivent être

253. - V.-L. Bénabou (présidente) et F. Langrognet (rapporteur), *Rapport de la mission du CSPLA sur les « œuvres transformatives »*, préc., p. 41.

254. - Art. L. 121-1 CPI : « L'auteur jouit du droit au respect de son nom, de sa qualité et de son œuvre. Ce droit est attaché à sa personne. Il est perpétuel, inaliénable et imprescriptible. Il est transmissible à cause de mort aux héritiers de l'auteur. L'exercice peut être conféré à un tiers en vertu de dispositions testamentaires ».

255. - Sur cette œuvre, V.supra, n°220.

256. - Cass. 1ère civ., 30 janv. 2007, n° 04-15.543.

257. - L. Vinogradoff, « Le créateur de Pepe The Frog tue sa grenouille, contaminée par l'extrême-droite », article *Le Monde Big Browser* du 8 mai 2017.

combattus a posteriori et sur le terrain judiciaire, mais le droit moral ne doit pas se transformer en régime d'autorisation a priori.

2 – L'exploitation du numérique

227. **La contre-attaque** - Dans les situations qui viennent d'être étudiées, la propriété littéraire et artistique résiste à des évolutions suscitées par les technologies numériques. Face aux possibilités de réaliser des copies privées, de poser des liens hypertextes, d'échanger des fichiers sur des réseaux de pair-à-pair, de transformer les œuvres existantes, elle ne s'écroule pas, ne désarme pas. Mieux : constatons à présent qu'elle transforme parfois l'ennemi numérique en allié, pour y découvrir de nouvelles sources de richesse (a), et de nouveaux moyens d'assurer sa protection (b).

a – Une protection étendue à de nouveaux objets

228. **Les logiciels**²⁵⁸ - Un dictionnaire usuel définit le logiciel comme « (l')ensemble des programmes, procédés et règles, et éventuellement de la documentation, relatifs au fonctionnement d'un ensemble de traitements de données »²⁵⁹. Sans ses logiciels, le matériel informatique — ordinateurs personnels, tablettes, serveurs... — est incapable de s'animer, et d'exécuter la moindre tâche au service de son utilisateur. Plusieurs couches de logiciels peuvent être distinguées. Le BIOS (*Basic Input/Output System*) est la plus fondamentale, en tant qu'elle assure les toutes premières phases de démarrage de la machine. Le système d'exploitation prend ensuite le relais. Il donnera lui-même la parole à des logiciels appliqués, dont la variété d'usages n'a pas d'autres frontières que celles de l'imagination humaine : bureautique, multimédia, jeux vidéo ou navigation Internet en constituent quelques catégories bien connues.

Un logiciel est écrit par un ou plusieurs programmeurs. Les plus sophistiqués — dont font partie les systèmes d'exploitation — fédèrent couramment les forces de centaines, voire de milliers de personnes. En vertu de préceptes déjà décrits, de tels objets intellectuels requièrent des investissements, et l'investissement suppose la protection par la propriété. Tel est du moins le paradigme classique, dont nous verrons plus loin qu'il est nuancé par les logiciels fonctionnant sous une « licence libre » : mais reconnaître à tous le droit gratuit d'exploiter et de modifier sa création, c'est encore, à certains égards, agir comme un propriétaire.

258. - Nous exploitons ici certains développements de notre contribution « Le logiciel dématérialisé » in *Les biens numériques*, éd. Ceprisca, 2014, p. 149.

259. - Dictionnaire Larousse en ligne, V° « Logiciel ».

Si l'on accepte le postulat selon lequel il convient d'accorder aux créateurs de logiciels un pouvoir exclusif sur leur chose — quitte à ce qu'il soit immédiatement relâché en certaines hypothèses -, la principale question qui reste à résoudre est celle de la forme que doit prendre cette protection par le droit. En effet, lorsque la question de la protection des créateurs de logiciels a commencé à se poser, dans les années 60, la doctrine hésitait entre deux solutions : faire basculer le logiciel dans le monde des brevets, en tant qu'il appartient « au monde de l'industrie et de la technique »²⁶⁰, ou le soumettre au droit d'auteur, en tant qu'œuvre de l'esprit. Le législateur français a opté pour la seconde solution. Aux termes de l'article L. 111-2 du Code de la propriété intellectuelle : « Sont considérés notamment comme œuvres de l'esprit au sens du présent code : [...] 13° Les logiciels, y compris le matériel de conception préparatoire [...] »²⁶¹. Si la loi française accorde au logiciel une protection directe, sans passer par le truchement de catégories préexistantes, la directive européenne de 1991 « concernant la protection juridique des programmes d'ordinateur »²⁶² a fait un autre choix. L'article 1er dispose en effet : « [...] les États membres protègent le programmes d'ordinateur par le droit d'auteur **en tant qu'œuvres littéraires** au sens de la convention de Berne pour la protection des œuvres littéraires et artistiques [...] »²⁶³. Certains ironisent : « [...] le logiciel se trouve ainsi placé quelque part entre Proust et Hemingway [...] »²⁶⁴. Qu'il soit considéré pour lui-même ou comme un cousin étrange de *La recherche du temps perdu*, le logiciel est donc placé sous l'égide du droit de la propriété littéraire et artistique. Ce choix continue à faire débat²⁶⁵. La jurisprudence, elle, est claire, depuis 1986 et un arrêt *Atari* de la Cour de cassation, dans lequel on peut lire : « [...] un logiciel, dès lors qu'il est original, est une œuvre de l'esprit protégée par la loi sur le droit d'auteur »²⁶⁶.

260. - C. Caron, *Droit d'auteur et droits voisins*, op. cit., n° 176.

261. - Cette protection du logiciel par le droit français a été initiée par la loi n° 85-660 du 3 juillet 1985 relative aux droits d'auteur et aux droits des artistes-interprètes, des producteurs de phonogrammes et de vidéogrammes et des entreprises de communication audiovisuelle.

262. - Directive n° 91/250 du 14 mai 1991.

263. - Art. 1er de la directive. Nous soulignons.

264. - M. Vivant et J.-M. Bruguière, *Droit d'auteur et droits voisins*, op. cit., n° 156. Les auteurs expliquent ce choix. Alors que le droit français accepte le principe d'une protection pour toute œuvre de l'esprit (art. L. 111-1 CPI), les pays de *copyright*, bien représentés en Europe, regroupent les œuvres susceptibles d'être protégées en une liste limitative. Il est alors plus facile de rattacher le nouvel arrivant à une catégorie préexistante.

265. - V. not. P. Catala, *Le droit à l'épreuve du numérique...*, op. cit., spéc. le chap. 15 : Le droit d'auteur sur les logiciels : protection banale ou spéciale ; J.-L. Goutal, « Logiciel : l'éternel retour », in *Droit et techniques. Etudes à la mémoire du professeur Xavier Linant de Bellefonds*, Lexisnexus, 2007, p. 217 ; C. Le Stanc, « Logiciel : trente ans entre droit d'auteur et brevet. Bilan ? », *Ibid.*, p. 272.

266. - Cass. ass. plén., 7 mars 1986, n° 84-93509 : Bull. ass. plén., n° 4 ; D. 1986, jur., p. 405, note B. Edelman ; JCP G, 1986, II, 20631, note J.-M. Mousseron, B. Teyssié et M. Vivant ; RTD. com., 1986, p. 399, obs. A. Françon ; RIDA, 1986, n° 129, p. 136, note A. Lucas.

La CJUE a eu l'occasion de préciser le périmètre exact de cette protection²⁶⁷. Le droit d'auteur ne protège pas les langages de programmation ni les fonctionnalités du programme²⁶⁸. En revanche, le code lui-même est protégé, aussi bien sous la forme du « code source » — le code tel qu'il est écrit et manipulé par les programmeurs — que sous la forme du « code objet » - qui résulte d'une transformation du code source en un matériau directement exploitable par la machine²⁶⁹. Un auteur souligne : « [...] il s'agit là d'une anomalie et d'une véritable entorse aux principes fondamentaux de la discipline. Le droit d'auteur devrait toujours protéger des formes d'expression perceptibles par des sens humains. L'exemple du code objet nous prouve que ce n'est pas toujours le cas et que le logiciel demeure un corps étranger en droit d'auteur »²⁷⁰.

Ainsi une richesse numérique considérable est-elle saisie par la propriété littéraire et artistique, au prix d'une distorsion importante de ses concepts.

229. Les bases de données - Dans un dictionnaire usuel, les termes « base de données » revêtent deux sens distincts. Le sens premier est un « un ensemble structuré de fichiers regroupant des informations ayant certains caractères en commun ». Le second est un « logiciel permettant de consulter et de gérer ces fichiers »²⁷¹. De même que le droit des données à caractère personnel est susceptible de concerner des fichiers papier, le droit de propriété intellectuelle sur les bases de données peut concerner un système de fiches bristol²⁷². Il est pourtant vain de nier l'écrasant principe sous prétexte de fugaces exceptions : c'est bien de numérique qu'il est ici question en tout premier lieu.

Au sens cette fois-ci du Code de la propriété intellectuelle : « On entend par base de données un recueil d'œuvres, de données ou d'autres éléments indépendants, disposés de manière systématique ou méthodique, et individuellement accessibles par des moyens électroniques ou par tout autre moyen »²⁷³. En revanche, le deuxième sens proposé par le dictionnaire usuel ne se retrouve pas ici : il est postulé que le logiciel permettant l'exploitation de la base de données est détachable de la base

267. - CJUE, 2 mai 2012, *SAS Institute Inc. c./ World Programming Ltd*, C-406/10.

268. - Dispositif de l'arrêt précité, 1). Comme l'écrit C. Caron, *op. cit.* n° 179 : « [...] un langage de programmation n'est qu'une succession de méthodes ou de données brutes, insusceptibles d'être protégées ».

269. - L'arrêt précité fonde la protection des deux formes du code sur l'article 9 de l'accord sur les aspects des droits de propriété intellectuelle qui touchent au commerce), figurant à l'annexe 1 C de l'accord de Marrakech instituant l'Organisation mondiale du commerce, qui a été approuvé par la décision 94/800/CE du Conseil, du 22 décembre 1994, relative à la conclusion au nom de la Communauté européenne.

270. - C. Caron, *op. cit.*, n° 180.

271. - Larousse en ligne, V° « Base de données ».

272. - Sur le traitement des données à caractère personnel, V. *supra*, n° 48 s.

273. - Art. L. 112-3 al. 2 CPI.

elle-même, et qu'il peut être protégé distinctement, ce qui ne semble pas correspondre à la réalité technique, qui fusionne largement ces deux aspects²⁷⁴.

Une base de données est un moyen d'organiser et de manipuler l'information : elle est donc la source d'un immense pouvoir. Il n'est pas exclu, lorsqu'elle présente une originalité suffisante, qu'elle soit protégée en application des principes habituels du droit d'auteur²⁷⁵. Mais la grande masse des bases de données, qui ne satisferait pas à ces exigeantes conditions, trouve ailleurs un refuge : dans un droit sui generis, conçu spécifiquement pour elles²⁷⁶.

*Le producteur d'une base de données, entendu comme la personne qui prend l'initiative et le risque des investissements correspondants, bénéficie d'une protection du contenu de la base lorsque la constitution, la vérification ou la présentation de celui-ci atteste d'un investissement financier, matériel ou humain substantiel*²⁷⁷.

Le numérique, une fois de plus, a provoqué en droit d'auteurs et droits voisins l'adoption de mesures d'exception. En effet, « [...] il s'agit d'une consécration sans précédent d'une protection directe de l'investissement en droit de la propriété intellectuelle »²⁷⁸. Habituellement, ce sont des résultats qui déclenchent la protection, tandis qu'on s'attache ici aux moyens qui ont été déployés.

Le régime juridique de ce droit sui generis est très complexe, et ne sera pas abordé ici. Il est organisé autour d'un monopole conféré au producteur de la base de données, qui lui donne le droit d'interdire « l'extraction » ainsi que la « réutilisation » « d'une partie qualitativement ou quantitativement substantielle » du contenu de la base²⁷⁹. L'extraction est un « transfert permanent ou temporaire [...] du contenu d'une base de données sur un autre support [...] », tandis que la réutilisation consiste en « [...] la mise à la disposition du public (..) du contenu de la base [...] »²⁸⁰. Ce qui est protégé, c'est bien l'agencement de l'information et non l'information elle-même : à preuve, une base de données contenant des informations relevant du domaine public bénéficiera du monopole²⁸¹.

274. - M. Vivant et J.-M. Bruguière, *op. cit.*, n° 216 in fine.

275. - C. Caron, *op. cit.*, n° 623, qui relève les dispositions de l'article L. 341-1 al. 2 CPI : « [La protection spéciale] est indépendante et s'exerce sans préjudice de celles résultant du droit d'auteur ou d'un autre droit sur la base de données ou un de ses éléments constitutifs ».

276. - Il est issu de la loi n° 98-536 du 1er juillet 1998 portant transposition dans le code de la propriété intellectuelle de la directive 96/9/CE du Parlement européen et du Conseil, du 11 mars 1996, concernant la protection juridique des bases de données.

277. - Art. L. 341-1 al. 1 CPI.

278. - C. Caron, *op. cit.*, n° 623.

279. - Art. L. 342-1 CPI. L'extraction est définie par ce texte comme un « La notion de "partie qualitativement ou quantitativement substantielle" est difficile à cerner : C. Caron, *op. cit.* n° 628.

280. - Même texte.

281. - C. Caron, *op. cit.*, n° 623.

À l'ère du *big data*, il ne faut pas sous-estimer la valeur économique considérable des bases de données²⁸². Elles sont le cœur battant de nombreux géants des activités en ligne, qui font rémunérer leurs services non par un prix en argent, mais par un transfert d'informations qui sont ensuite organisées avec soin, puis exploitées.

La propriété intellectuelle ayant procédé aux contorsions nécessaires pour se saisir des nouvelles richesses numériques, il lui restait à exploiter les technologies de l'information à des fins défensives.

b – Une protection renforcée par de nouveaux moyens

230. Les mesures techniques de protection « bloquantes » - En évoquant le destin de l'exception de copie privée à l'ère numérique, nous avons rappelé que les nouvelles technologies s'étaient présentées, dans un premier temps, comme une terrible menace pour l'univers de la propriété littéraire et artistique. Un monde de copies parfaites, presque gratuites et quasi instantanées est un monde où les objets culturels circulent de manière incontrôlable, croyait-on. Qu'on y voie une menace — que disparaissent les incitations à produire des œuvres de l'esprit — ou une chance — d'abolir les obstacles matériels, financiers, géographiques à la circulation de la créativité humaine — est ensuite affaire de politique. Mais ce paradigme est dépassé : il correspondait à un premier état de la technique. D'adversaire, le numérique s'est peu à peu mué en un puissant allié du droit d'auteur, grâce aux mesures techniques de protection (les MTP). Ce phénomène a été très largement analysé par la doctrine de propriété intellectuelle, ce qui nous permet de nous limiter à en donner un aperçu d'ensemble²⁸³.

C'est un lieu commun que de comparer les MTP à un cadenas ou à une barrière²⁸⁴. Si quelqu'un tente de braver la loi qui interdit de pénétrer sans autorisation sur la propriété privée d'autrui, un obstacle matériel s'opposera à la liberté d'action du délinquant en puissance, et le contraindra à l'abandon. De même, un autoradio peut être conçu de manière à cesser de fonctionner s'il est débranché sans autorisation du véhicule dans lequel il avait été initialement installé²⁸⁵. Il ne reste plus qu'à imaginer que l'appareil dirige ses contrôles non pas vers l'automobile à laquelle il est branché, mais en direction des CD audio qu'on y insère, afin de déceler des reproductions non autorisées par le titulaire des droits, et l'on découvre une première forme de MTP. On peut la

282. - Sur la notion de *big data*, V. supra, n°55.

283. - V. not. S. Dusollier, *Droit d'auteur et protection des œuvres dans l'univers numérique*, Larcier, 2005.

284. - Par ex. C. Caron, *op. cit.*, n° 333. S. Dusollier estime dans le même ordre idées que des « clôtures technique » s se superposent aux « clôtures juridiques » (*op. cit.*, n° 25).

285. - L. Lessig, *Code V2*, *op. cit.*, p. 126.

qualifier de « bloquante » : elle ouvre ou ferme un accès, permet ou empêche un fonctionnement, de même que le cadenas laisse passer celui qui possède une clé et s'oppose à ceux qui n'en ont pas. À ce stade, plusieurs questions méritent déjà d'être posées.

231. Qui protégera les protecteurs²⁸⁶ ? - Une serrure peut être forcée ; une MTP peut être contournée. Mais déjà l'analogie montre des limites. Dans le cas d'une effraction, la victime se plaindra d'une atteinte à sa propriété, c'est-à-dire qu'elle invoquera le droit sous-jacent que la pose d'un loquet n'avait vocation qu'à renforcer. Le « bris de serrure » n'est une infraction en lui-même que parce qu'un objet matériel appartenant autrui a été dégradé. Celui qui parvient à lire un CD contrefait sur un autoradio qui devrait y être rétif n'a pas « détruit » la MTP : généralement, il ne se sera agi que de tromper un logiciel - fût-ce un logiciel rudimentaire. Si l'analogie était exacte, les poursuites éventuelles ne pourraient se fonder que sur l'atteinte au droit sous-jacent, c'est-à-dire sur la contrefaçon. Or, il existe en propriété littéraire et artistique un dispositif, souvent qualifié de « para-contrefaçon », qui protège les MTP en tant que telles : un droit des serrures immatérielles. L'intérêt est double. D'abord, contourner une MTP laisse des traces, produit des preuves qui ne sont pas les mêmes que celles qui résultent, par la suite, de la simple utilisation contrefaisante d'œuvres de l'esprit. En incriminant directement le comportement préparatoire à la contrefaçon, on augmente les chances de parvenir à une condamnation²⁸⁷. Ensuite, cela permet d'incriminer le comportement qui consisterait à vendre ou à offrir des moyens de contourner des MTP, et même la simple proposition de le faire²⁸⁸.

232. Le problème de l'efficacité excessive - Si les MTP épousaient parfaitement les contours de ce qu'interdisent droit d'auteur et droits voisins, s'il ne s'agissait que de mettre dans la main de la loi le glaive de la technique, il n'y aurait pas lieu de se plaindre. Mais la coïncidence n'est pas parfaite. L'arrêt *Mulholland drive*, déjà évoqué, en constitue l'illustration la plus fameuse. L'acheteur d'un DVD de ce film souhaitait en réaliser une copie privée, à destination de son cercle

286. - Paraphrase de la fameuse question qui conclut le *comic Watchmen* d'A. Moore et D. Gibbons : « *who watches the Watchmen ?* ».

287. - Art. L. 335-3-1 CPI, I : « est puni de 3 750 euros d'amende le fait de porter atteinte sciemment, à des fins autres que la recherche, à une mesure technique efficace telle que définie à l'article L. 331-5, afin d'altérer la protection d'une œuvre par un décodage, un décryptage ou toute autre intervention personnelle destinée à contourner, neutraliser ou supprimer un mécanisme de protection ou de contrôle, lorsque cette atteinte est réalisée par d'autres moyens que l'utilisation d'une application technologique, d'un dispositif ou d'un composant existant mentionné au II ».

288. - Même texte, II : « Est puni de six mois d'emprisonnement et de 30 000 euros d'amende le fait de procurer ou proposer sciemment à autrui, directement ou indirectement, des moyens conçus ou spécialement adaptés pour porter atteinte à une mesure technique efficace telle que définie à l'article L. 331-5, par l'un des procédés suivants [...] ».

de famille, comme l'y autorise apparemment une exception au droit d'auteur²⁸⁹. Or, des MTP insérées dans le support rendaient impossible toute reproduction de l'œuvre. La Cour décide que :

[...] l'atteinte à l'exploitation normale de l'œuvre, propre à faire écarter l'exception de copie privée s'apprécie au regard des risques inhérents au nouvel environnement numérique quant à la sauvegarde des droits d'auteur et de l'importance économique que l'exploitation de l'œuvre, sous forme de DVD, représente pour l'amortissement des coûts de production cinématographique [...].

Aurait-on confondu *exception* au droit d'auteur et *droit* à réaliser des copies privées ? Ce n'est pas si simple. Le droit européen oblige les États membres à garantir l'effectivité de certaines exceptions en dépit de la présence de MTP - par exemple, les reproductions effectuées par les bibliothèques, établissements d'enseignement, musée ou archives²⁹⁰. Pour la copie privée, ils en ont simplement la faculté. Pour d'autres encore, ils sont libres d'agir comme ils l'entendent, sans que rien ne permette véritablement à la doctrine de savoir comment ces trois catégories ont été définies²⁹¹.

Si la Haute autorité pour la diffusion des œuvres et la protection des droits sur Internet est bien connue dans son rôle de lutte contre la contrefaçon sur les réseaux de pair-à-pair, le grand public connaît moins le rôle de « veille et de régulation » en matière de MTP qui lui a été confié par la loi²⁹². C'est à elle que revient notamment la protection des exceptions contre les verrous techniques excessifs²⁹³.

233. Le para-droit des MTP intelligentes - Jusqu'ici, les MTP étaient présentées comme une porte qui s'ouvre ou se ferme, éventuellement percées de quelques trous pour laisser filtrer la lumière des exceptions au droit d'auteur légalement protégées. En l'état de la technique, le système n'est plus aussi binaire. La définition légale de ces protections le révèle : « Les mesures techniques efficaces destinées **à empêcher ou à limiter les utilisations non autorisées** par les titulaires d'un droit d'auteur ou d'un droit voisin du droit d'auteur d'une œuvre [...] »²⁹⁴. Il peut donc s'agir de

289. - Cass., 1ère civ., 28 févr. 2006, n° 05-15.824 : V.supra, n°213.

290. - Directive 2001/29/CE du 22 mai 2001, précitée, article 6.4.

291. - A. Latreille et T. Maillard, « Mesures techniques de protection et d'information », fasc. 1660 in *J-Classeur Propriétaire littéraire et artistique*, 16 février 2015, n° 160.

292. - Art. L. 331-31 et s. CPI. Sur le rôle de lutte contre le téléchargement illégal sur les réseaux P2P, V.supra, n°215.

293. - V. par ex. son avis n° 2014-1 relatif à l'exception de copie privée des programmes télévisés. Il a permis que les enregistrements réalisés par l'intermédiaire de « boxes » Internet prennent la forme de fichiers exportables, par exemple vers un ordinateur.

294. - Art. L. 331-5 CPI. Précisons que ce texte écarte les logiciels de son champ d'application, tout simplement parce qu'ils étaient déjà protégés par des dispositions plus anciennes (V. not. art. L. 122-6-2 CPI). Cela n'a guère d'impact sur le sens général de la démonstration.

simplement « limiter » les utilisations de l'œuvre. Le noir et le blanc sont donc rejoints par une infinité de nuances de gris.

La sophistication des MTP se traduit aussi bien au stade de la détection des utilisations non autorisées qu'au stade de la réaction qui s'enclenche alors. Le *Audio Home Recording Act* américain déjà évoqué, en fournit une illustration vieille d'un quart de siècle²⁹⁵. Au stade de la détection : les appareils susceptibles de réaliser des copies audio numériques n'interdisaient pas radicalement de dupliquer une œuvre, mais comptaient les reproductions réalisées. Au stade de la réaction : les copies surnuméraires n'étaient pas empêchées, mais leur qualité était volontairement dégradée.

Lawrence Lessig propose un exemple de contrôle encore bien plus fin, parce que plus récent, avec le système de permissions accordées par le logiciel de lecture de livres électroniques *Adobe eBook Reader*²⁹⁶. L'auteur prend un livre précis comme exemple et révèle les autorisations qui lui sont accordées. Il peut ainsi copier-coller dix passages dans la mémoire de son ordinateur par tranche de dix jours. Au cours de la même période, il ne peut imprimer plus de dix pages. Il s'agit pourtant d'un texte... tombé dans le domaine public²⁹⁷.

L'image du verrou posé sur la porte est donc très réductrice. L'expression anglaise de *Digital rights management*, parfois traduite en « gestion numérique des droits », semble mieux rendre compte de la réalité que celle de « mesures techniques de protection ». Les instruments dont il s'agit n'ont pas seulement vocation à protéger l'œuvre : ils sont un moyen de la distribuer avec un degré de contrôle qui n'a jamais connu d'équivalent. Par exemple, Il devient possible de facturer l'utilisateur, chez lui, à la page de journal lue ou à la minute de musique écoutée, au fur et à mesure de la consommation. L'accès à l'œuvre peut être octroyé de manière complète, à titre de démonstration, pour un court laps de temps, avant d'être entièrement retiré. Un livre peut être « acheté », dans lequel le lecteur ne pourrait jamais revenir en arrière.

Certaines MTP doivent donc être considérées aujourd'hui comme de véritables systèmes normatifs embarqués : un ensemble complexe de règles les accompagne, et, de surcroît, possède une capacité à s'auto-exécuter sans qu'il soit nécessaire de recourir à une assistance extérieure. L'aphorisme « Code is law », descriptif et non prescriptif, prend ici son sens le plus fort²⁹⁸. Or, ce système normatif embarqué peut venir en renfort de la loi — par exemple, en empêchant la contrefaçon d'une œuvre protégée –, mais aussi poser des règles tolérées par la loi sans être prévues

295. - V.supra, n°213.

296. - L. Lessig, *Free culture*, op. cit., p. 148.

297. - En l'occurrence, *Middlemarch* de George Eliot. Pire : l'auteur constate ensuite qu'il n'a droit à aucun copier-coller ni aucune impression papier

298. - La formule est de L. Lessig et figure notamment dans *Code V2*, op. cit.

par elle — l'interdiction de réaliser une copie privée -, voire aller directement à l'encontre de la loi - en empêchant le libre usage d'un texte tombé dans le domaine public²⁹⁹. Le truchement du contrat semble au premier abord autoriser l'harmonie, le titulaire du droit ayant à la fois le contrôle du contenu du contrat d'adhésion permettant l'accès à l'œuvre et le contrôle des règles gouvernant la MTP. Mais la convention pourrait être contraire à l'ordre public. Un autre cas de figure doit être mentionné, qui se présentera fréquemment : celui dans lequel les MTP profitent du silence des textes, la loi ayant été conçue à une époque où il n'était pas possible d'imaginer qu'un tel degré de contrôle serait conféré aux titulaires d'un droit d'auteur. Nous ouvrirons plus loin ce débat, lorsqu'au droit de propriété sur les œuvres, certains tenteront d'opposer un droit du consommateur de produit culturel sur son exemplaire de l'œuvre.

234. **Les « robocopyrights »** - Les systèmes de « tatouage numérique » des œuvres protégées par le droit d'auteur constituent un cas particulier de MTP qui fait l'objet de controverses particulièrement vives : il convient donc d'en dire quelques mots.

À l'occasion de l'étude de la liberté d'expression sur Internet, avaient été rappelées les dispositions de la loi pour la confiance dans l'économie numérique relatives aux intermédiaires, selon lesquelles ces plateformes :

*[...] ne peuvent pas voir leur responsabilité civile engagée du fait des activités ou des informations stockées à la demande d'un destinataire de ces services si elles n'avaient pas effectivement connaissance de leur caractère illicite ou de faits et circonstances faisant apparaître ce caractère ou si, dès le moment où elles en ont eu cette connaissance, elles ont agi promptement pour retirer ces données ou en rendre l'accès impossible*³⁰⁰.

Nous précisons que le Conseil constitutionnel a restreint l'obligation d'agir faite aux intermédiaires aux situations « manifestement » illicites³⁰¹. En matière de propriété intellectuelle, cela suppose que les auteurs de notifications apportent aux intermédiaires la preuve qu'ils sont titulaires du droit bafoué, accompagnée du constat de la violation³⁰². La loi commande donc une

299. - La doctrine américaine évoque un *private ordering* : S. Dussolier, *op. cit.*, n° 269. Adde M. Vivant et J.-M. Bruguère, *op. cit.*, n° 969. Ces auteurs soulignent que cette privatisation « [...] ne devrait pas laisser indifférent un législateur soucieux de l'exercice d'un droit d'auteur démocratique. Mais qui ne signifie pas la mort du droit d'auteur ». Le droit d'auteur, rappellent-ils, a su s'adapter par le passé à des évolutions technologiques qui pouvaient sembler, aux yeux de leurs contemporains, tout aussi radicales.

300. - Art. 6, I, 2 de la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique. Sur l'application de ce texte aux abus de la liberté d'expression, V.supra, n°161.

301. - Décision n° 2004-496 DC du 10 juin 2004, considérant n° 9. Il n'y pas à rechercher si cette condition est remplie lorsqu'un ordre judiciaire de retrait a été donné. V.supra, n°163.

302. - L. Marino, « Responsabilité civile et pénale des fournisseurs d'accès et d'hébergement » fasc. 670, in *J.-Cl. Communication*, n° 49, s'appuyant sur CA Paris, 14e ch., 12 déc. 2007, n° 071036 : *LDI*, 2008, n° 35, 1164, note L. Thoumyre.

réaction curative, mais n'ordonne pas d'attitude préventive. Cependant, de fait, nombreuses sont les plateformes susceptibles d'héberger du contenu en violation du droit d'auteur à avoir mis en place des systèmes « d'empreintes numériques ». Comme l'explique par exemple YouTube :

Les vidéos mises en ligne sur YouTube sont comparées à une base de données de fichiers fournis par les propriétaires de contenu. Ce sont eux qui décident de la procédure à suivre lorsqu'une correspondance est établie entre une vidéo mise en ligne sur YouTube et leur propre contenu. Dans ce cas de figure, la vidéo en question fait l'objet d'une revendication Content ID³⁰³.

Ce seul système revendique « plus de 50 millions de fichiers de référence actifs »³⁰⁴. L'avantage de ce système est évident : avec 400H de vidéos versées sur YouTube chaque minute, la masse de contenus à analyser dépasse les capacités humaines, mais n'effraie pas les robots³⁰⁵. Mais les inconvénients d'une telle démarche sont tout aussi patents. Ils résultent, là encore, d'une discordance entre le contenu de la loi et le contenu normatif embarqué dans la MTP. La mesure de protection est construite sur le modèle : « si une trace d'un contenu sous droit est détectée, considérer la vidéo qui l'utilise comme interdite ». La loi, cela a déjà été exposé lors de l'étude des usages transformatifs, est bien plus nuancée. Des fragments de l'œuvre peuvent être utilisés lorsqu'ils sont d'une importance négligeable³⁰⁶. Il existe des exceptions au droit d'auteur qui s'appliquent à des extraits vidéo, notamment la parodie³⁰⁷. Le robot n'en tient aucun compte.

L'artiste Mozinor raconte ainsi comment, il y a quelques années, sa parodie du film Titanic a entraîné non seulement la suppression de sa vidéo, mais également la fermeture complète de sa chaîne YouTube³⁰⁸. Récemment, ayant constaté qu'un autre humoriste avait exploité les mêmes images du même film, il a tenté de remettre son montage sur la plateforme. Il en a été retiré à nouveau. Avec l'aide d'un juriste, il a déposé une réclamation qui a permis le retour de son œuvre... pendant une heure, après quoi elle a de nouveau été retirée³⁰⁹.

Le problème est tel qu'il a poussé la mission « œuvres transformatives » du CSPLA à formuler une préconisation sur ce sujet, qui se situe pourtant à la périphérie de son objet d'étude :

303. - <https://support.google.com/YouTube/answer/2797370?hl=fr>.

304. - <https://www.YouTube.com/intl/fr/yt/about/press/>.

305. - Le chiffre est tiré de <http://www.webrankinfo.com/dossiers/YouTube/chiffres-statistiques>.

306. - Sur cette approche « de minimis », V.supra, n°221.

307. - *Ibid.*

308. - Mozinor, « Titanic strike » : <https://www.YouTube.com/watch?v=yixx6vqYR9U>. Le terme « strike » désigne le fait, pour le robot, de retirer une vidéo de la plateforme. La vidéo retirée est celle-ci : http://www.dailymotion.com/video/x1jml6_titanic-park_creation.

309. - Le juriste en question est L. Maurel, dont on peut lire le commentaire : « Liberté d'expression : le Web européen subira-t-il la “malédiction du Titanic ?” », article *scinfolex.com* du 30 avril 2017.

*Préconisation 2 : Développer des procédures simples, rapides et contradictoires afin de remédier aux blocages intempestifs des créations transformatives légitimes par certains systèmes de tatouage numérique. Encourager les processus de médiation pour résorber les conflits et assurer la présence des œuvres transformatives légitimes sur le réseau*³¹⁰.

Dans ce contexte, le projet de directive droit d'auteur ne peut qu'interpeller. Il est ainsi prévu que :

*Les prestataires de services de la société de l'information qui stockent un grand nombre d'œuvres ou d'autres objets protégés chargés par leurs utilisateurs et qui donnent accès à ces œuvres et autres objets prennent, en coopération avec les titulaires de droits, des mesures destinées à assurer le bon fonctionnement des accords conclus avec les titulaires de droits en ce qui concerne l'utilisation de leurs œuvres ou autres objets protégés ou destinées à empêcher la mise à disposition, par leurs services, d'œuvres ou d'autres objets protégés identifiés par les titulaires de droits en coopération avec les prestataires de services. Ces mesures, **telles que le recours à des techniques efficaces de reconnaissance des contenus**, doivent être appropriées et proportionnées [...]*³¹¹.

Rendre obligatoires des dispositifs qui ont démontré leurs effets pervers peut inquiéter. Il est vrai que les grandes plateformes les appliqueront quoiqu'il arrive, sur la base de contrats passés avec les titulaires de droits³¹². Les plus optimistes remarqueront que le projet de directive rend obligatoires « des dispositifs de plainte et de recours à l'intention des utilisateurs pour les litiges relatifs » au fonctionnement de ces MTP³¹³. Toutefois, mettre ces procédures en place ne sert à rien si elles se révèlent aussi ineffectives que dans l'affaire Mozinor.

235. La propriété triomphante ? - Le numérique n'a pas tué la propriété littéraire et artistique. Celle-ci a cédé fort peu de terrain face aux réseaux de pair-à-pair, aux liens hypertextes ou à l'explosion des pratiques transformatives : ses principes fondateurs ont résisté, quitte à créer parfois d'importants frottements avec la réalité des pratiques sociales. Le droit d'auteur s'est même livré à une impressionnante contre-attaque : il a su trouver dans l'univers numérique de nouvelles richesses à exploiter, considérables. Il a surtout recruté pour l'assister des sentinelles techniques qui menacent, par un surprenant choc en retour, de donner à la propriété des objets culturels une puissance excessive.

Ces constats doivent à présent être nuancés : la progression du numérique a parfois été l'occasion d'un certain relâchement de la propriété des œuvres de l'esprit.

310. - V.-L. Bénabou (présidente) et F. Langrognet (rapporteur), *Rapport de la mission du CSPLA sur les « œuvres transformatives »*, préc., p. 29.

311. - Article 13.1 de la proposition de directive sur le droit d'auteur dans le marché unique numérique, précitée.

312. - L'intérêt pour les plateformes est que le titulaire du droit, une fois prévenu de la présence d'une vidéo prétendument contrefaisante, pour choisir de demander à être associé aux gains publicitaires plutôt que de la faire retirer :supra, n°222.

313. - Art. 13.2 de la proposition de directive sur le droit d'auteur dans le marché unique numérique, précitée.

B - La propriété tempérée

236. **Sources des assouplissements** - La puissance du rôle joué par la propriété en matière de contenus numériques a été modérée tantôt sur ordre de la loi (1), tantôt par le pouvoir de la volonté (2).

1 - Les tempéraments légaux

237. **Les copies provisoires et techniques** - Pour qu'une œuvre protégée par le droit d'auteur soit consultable sur Internet, les informations qui la constituent doivent voyager du serveur qui la contient jusqu'à un terminal client - ordinateur, tablette, téléphone intelligent... Pour cela, de multiples copies de cette œuvre doivent être réalisées. On peut laisser de côté le voyage des différents « paquets » d'information sur les réseaux de télécommunication, car ils voyagent en principe sous la forme de fragments dénués de sens, qui peuvent emprunter des chemins distincts, avant d'être reconstitués en aval. En revanche, des copies de l'œuvre pourront être réalisées par des moteurs de recherche aux fins d'indexation, par des serveurs « proxys » — qui stockent les informations les plus fréquemment consultées au plus près des utilisateurs, afin d'éviter d'aller les chercher à chaque fois sur leur serveur d'origine, plus distant -, dans la mémoire cache du navigateur de l'utilisateur et sur son écran. Comme l'écrit M. Lessig :

Digital technology, at its core, makes copies. Copies are to digital life as breathing is to our physical life. There is no way to use any content in a digital context without that use producing a copy. When you read a book stored on your computer, you make a copy (at least in the RAM memory to page through the book). When you do anything with digital content, you technically produce a copy³¹⁴.

Dans une vision éthérée et maximaliste du monopole de l'auteur, ces actes de reproduction pourraient être soumis à autorisation. Mais l'abstraction que constitue la réservation des utilités de l'œuvre au profit de son créateur doit rencontrer des limites, lorsque sa mise en œuvre entraînerait une régression technologique généralisée sans qu'aucun bien-être social n'en résulte en contrepartie. Ouvrir un débat sur la licéité d'un lien hypertexte créé sur un blog et pointant vers la page d'accueil du *Monde*, en tant qu'il constitue une communication au public d'œuvres protégées par le droit d'auteur, a déjà de quoi troubler les non-juristes³¹⁵. Qu'une autorisation de l'ensemble des créateurs concernés soit nécessaire pour afficher ce site sur un écran et le stocker un disque dur, provisoirement, n'aurait pas de sens. C'est pourquoi la loi autorise :

6° La reproduction provisoire présentant un caractère transitoire ou accessoire,

314. - L. Lessig, *Code V2*, op. cit., p. 192.

315. - V.supra, n°216.

*lorsqu'elle est une partie intégrante et essentielle d'un procédé technique et qu'elle a pour unique objet de permettre l'utilisation licite de l'œuvre ou sa transmission entre tiers par la voie d'un réseau faisant appel à un intermédiaire ; toutefois, cette reproduction provisoire qui ne peut porter que sur des œuvres autres que les logiciels et les bases de données ne doit pas avoir de valeur économique propre*³¹⁶.

Certains auteurs estiment même qu'il ne s'agit pas d'une véritable exception : « Intellectuellement, il paraît bien que l'on n'est pas dans le périmètre du droit, car ces reproductions sont strictement fonctionnelles. Il serait aberrant de morceler le processus de communication en de multiples faits de reproduction dénués de réalité propre »³¹⁷.

Les copies techniques constituent une entaille dans le droit de propriété de l'auteur, ou bien elles se situent plus radicalement hors de son orbe. Elles sont quoi qu'il en soit indispensables.

238. La fouille de données - Si l'exception pour copies techniques est une nécessité, celle qui concerne la fouille de données est un choix. Si la première constitue un simple soubassement juridique du fonctionnement normal des technologies numériques, la seconde permet d'en tirer le plein potentiel dans le cadre de la recherche scientifique.

Le *Text and Data Mining* peut être défini comme un « traitement automatisé de contenus numériques [...] afin de découvrir de nouvelles connaissances ou des idées »³¹⁸. Soit un chercheur qui découvrirait, sur le site d'un grand éditeur scientifique, une gigantesque mine d'informations qui pourrait livrer de multiples secrets, une fois balayée en tous sens par les algorithmes adéquats. Si la seule autorisation contractuelle prévue permet une consultation en direct sur un écran, la fouille sera impossible. Il est nécessaire qu'une copie durable puisse être réalisée, puis exploitée localement. La loi République numérique y a consenti, en posant une nouvelle exception au monopole de l'auteur, qui concerne :

*[...] Les copies ou reproductions numériques réalisées à partir d'une source licite, en vue de l'exploration de textes et de données incluses ou associées aux écrits scientifiques pour les besoins de la recherche publique, à l'exclusion de toute finalité commerciale [...]*³¹⁹.

Le texte est complété par une disposition relative au droit des bases de données³²⁰.

316. - Art. L. 122-5 CPI.

317. - M. Vivant et J.-M. Bruguière, *op. cit.*, n° 630.

318. - L. Ballet, « Text & Data Mining, l'impossible exception », *Dalloz IP/IT*, 2016, p. 415, citant un rapport remis à la Commission européenne en 2014 dans le cadre de l'évaluation juridique de l'UE en matière de droit d'auteur.

319. - Art. L. 122-5, 10° CPI, issu de la loi n° 2016-1321, précitée.

320. - Art. L. 342-3, 5° CPI. Les deux dispositions n'ont d'ailleurs pas été rédigées de manière tout à fait concordante, sans que cela s'explique : T. Azzi, « Open data et propriété intellectuelle. État des lieux au lendemain de l'adoption de la loi pour une République numérique », *D.*, 2017, p. 583.

Une nouvelle fois, le droit de propriété doit être mis en balance avec l'intérêt général, représenté ici par les bénéfices procurés à l'ensemble de la société par une recherche scientifique performante. Toutefois, le progrès réalisé en ce sens est encore timide : un auteur relève l'impossibilité de procéder à des fouilles de données non textuelles — sons, images, vidéos — ; l'exclusion des finalités commerciales, qui évince les partenariats public-privé du champ du dispositif ; l'absence de prise en compte, par le texte, de l'existence de MTP susceptibles de faire obstacle à la fouille³²¹.

Ces limites peuvent être nuancées par le caractère nécessairement provisoire du dispositif issu de la loi République numérique. Il semble en effet contradictoire avec le droit positif de l'Union, qui lui est hiérarchiquement supérieur : il s'agirait donc d'une législation d'anticipation ou de provocation³²².

Or, le projet de directive sur le droit d'auteur envisage bien de consacrer une nouvelle exception relative à la fouille de textes et de données³²³. De surcroît, elle ne serait pas restreinte aux seules œuvres textuelles ni limitées à des utilisations non commerciales.

239. La mise à disposition du public des résultats scientifiques - Dans le cadre de la fouille de textes et de données, les technologies numériques se présentaient comme un outil de travail scientifique. Mais elles peuvent également servir à la diffusion des produits de la recherche. Un mouvement dit de libre accès à la recherche — *open access* — s'est développé au niveau mondial, qui estime que l'utilité sociale des résultats scientifiques augmente significativement lorsque leur circulation est facilitée. Différentes barrières peuvent se dresser contre celui qui souhaite accéder à ces connaissances : elles peuvent être physiques — les publications papier nécessitent des déplacements, consommateurs de temps et de ressources — ou directement monétaires, lorsque se constituent de puissants oligopoles d'éditeurs dont les tarifs sont hors de contrôle.

Des outils numériques peuvent être employés pour octroyer à tous un accès instantané et gratuit à ces connaissances de haut niveau. Ils sont au cœur de l'*open access*. La création par le CNRS, en

321. - L. Maurel, « L'exception TDM dans la loi numérique : mérites, limites et perspectives », article *scinfolex.com* du 9 novembre 2016.

322. - En ce sens : T. Azzi, « Open data.... », art. préc.

323. - Proposition de directive sur le droit d'auteur dans le marché unique numérique du 14 septembre 2016, précitée, art. 3. : « Les États membres prévoient une exception aux droits visés à l'article 2 de la directive 2001/29/CE, à l'article 5, point a), et à l'article 7, paragraphe 1, de la directive 96/9/CE, et à l'article 11, paragraphe 1, de la présente directive pour les reproductions et extractions effectuées par des organismes de recherche, en vue de procéder à une fouille de textes et de données sur des œuvres ou autres objets protégés auxquels ils ont légitimement accès à des fins de recherche scientifique. 2. Toute disposition contractuelle contraire à l'exception prévue au paragraphe 1 est sans effet. 3. Les titulaires des droits sont autorisés à appliquer des mesures destinées à assurer la sécurité et l'intégrité des réseaux et bases de données où les œuvres ou autres objets protégés sont hébergés. Ces mesures n'excèdent pas ce qui est nécessaire pour atteindre cet objectif. 4. Les États membres encouragent les titulaires des droits et les organismes de recherche à définir d'un commun accord des bonnes pratiques concernant l'application des mesures visées au paragraphe 3 ».

2001, de la plateforme HAL — Hyper articles en ligne —, archive ouverte dans laquelle les chercheurs peuvent déposer leurs manuscrits en libre accès, constitua l'une des premières illustrations de cette démarche³²⁴.

Toutefois, la carrière des chercheurs, aussi bien en sciences dures qu'en sciences humaines, passe par la publication régulière de travaux dans des revues prestigieuses, dont la plupart relèvent du secteur privé. Pour accéder à leurs colonnes, ils cèdent aux éditeurs leur droit d'auteur, et se retrouvent alors privés de la possibilité de partager le fruit de leurs travaux en accès libre et gratuit.

Conscient de cette difficulté, le législateur français s'est inspiré du droit allemand pour conférer aux chercheurs un droit de mettre leur travail à disposition du public, nonobstant la cession de propriété à laquelle ils avaient consenti au profit d'un éditeur, à certaines conditions³²⁵.

Certains tempéraments au droit de propriété littéraire et artistique sont donc imposés par la loi. Mais il est des situations où c'est le titulaire du droit d'auteur lui-même qui décide d'un relâchement de l'emprise qui lui a été conférée sur son œuvre.

2. - Les tempéraments volontaires

240. Principe des licences libres - Le mouvement *d'open access*, dont il vient d'être question, s'appuie sur des outils numériques pour assurer une diffusion la plus large possible d'œuvres de l'esprit. Il est possible d'aller plus loin, et d'offrir au public la possibilité de procéder lui-même à de nouvelles publications de l'œuvre, pour en assurer une propagation virale, mais aussi et surtout d'y apporter des modifications. Mais le Code de la propriété intellectuelle, ainsi qu'il a été précédemment démontré, se prête malaisément à ces usages transformatifs³²⁶. Certes, il existe un domaine public, constitué des œuvres de l'esprit pour lesquelles les droits patrimoniaux de l'auteur ont expiré³²⁷. La réservation des utilités de l'œuvre au profit de l'auteur ne dure qu'un temps, après

324. - <https://hal.archives-ouvertes.fr/>.

325. - En droit allemand, V. le §15 de la loi sur le droit d'auteur, *Gesetz über Urheberrecht und verwandte Schutzrechte (Urheberrechtsgesetze)* : § 15 Allgemeines, (2) sur la communication au public sous forme immatérielle.

326. - V.supra, n° 219 s. Sur l'articulation des notions d'œuvre transformative et d'œuvre libre : M. Clément-Fontaine, « L'œuvre libre », fasc. 1975 in *J-Cl. Propriété littéraire et artistique*, 22 juillet 2014, n° 7, in fine.

327. - Les débats autour de la loi « République numérique » avaient permis d'envisager, un temps, que la loi consacre l'existence d'un « domaine public informationnel » constitué des « (...) informations, faits, idées, principes, méthodes, découvertes, dès lors qu'ils ont fait l'objet d'une divulgation publique licite, notamment dans le respect du secret industriel et commercial et du droit à la protection de la vie privée » ainsi que des « (...) œuvres, dessins, modèles, inventions, bases de données, protégés par le code de la propriété intellectuelle (...) dont la durée de protection légale, à l'exception du droit moral des auteurs, a expiré ». Cette proposition n'a finalement pas été retenue (M. Rees, « Loi numérique : les députés disent non au domaine commun informationnel », article *nextinpact.com* du 21 janvier 2016).

lequel les droits patrimoniaux se flétrissent, laissant seul subsister un droit moral éternel. La réservation est toutefois fort longue, puisqu'elle dure actuellement soixante-dix ans après la mort de l'auteur³²⁸. Le fonds culturel commun dans lequel chacun est libre de puiser se constitue donc selon un lent processus de sédimentation, qui dépasse le siècle pour des œuvres de jeunesse³²⁹.

Ce que la loi rechigne à faire, la volonté le peut-elle ? Relâcher sciemment son emprise exclusive, permettre à tous de profiter de son bien, c'est encore se comporter en propriétaire³³⁰. L'idée pourrait fort bien trouver application dans un contexte étranger au numérique, mais c'est pourtant là qu'elle est véritablement née et qu'elle se développe. Le développement du réseau a donné naissance à certaines communautés très attachées à l'idée de partage. Comme l'expose Madame Clément-Fontaine, l'informaticien Richard Stallmann a joué un rôle essentiel dans ce processus, en créant la *GNU General Public License* (GPL) et la *Free Software Foundation*, destinée à la promouvoir³³¹. Prenant place dans l'univers de la création de logiciels, ce contrat de licence est le premier qui organise non seulement les droits conférés aux licenciés directs, mais la pérennité des libertés ainsi accordées : celles-ci devront, à l'avenir, obligatoirement se transmettre de proche en proche à chaque utilisation de variantes de l'œuvre initiale, faisant grandir le fonds des biens communs informationnels³³². Sans cela, l'auteur d'une adjonction ou d'une transformation de l'œuvre initiale pourrait faire valoir la plénitude de ses droits d'auteur dans leur conception classique, et la chaîne de libertés serait brisée. Le Préambule de la version la plus récente explique ainsi :

To protect your rights, we need to prevent others from denying you these rights or asking you to surrender the rights. Therefore, you have certain responsibilities if you distribute copies of the software, or if you modify it: responsibilities to respect the freedom of others.

For example, if you distribute copies of such a program, whether gratis or for a fee, you

328. - Art. L. 123-1 CPI : « L'auteur jouit, sa vie durant, du droit exclusif d'exploiter son œuvre sous quelque forme que ce soit et d'en tirer un profit pécuniaire. Au décès de l'auteur, ce droit persiste au bénéfice de ses ayants droit pendant l'année civile en cours et les soixante-dix années qui suivent ».

329. - Par comparaison, L. Lessig explique comment Walt Disney a pu revisiter, dans ses œuvres, une culture constituée de toute œuvre publiée depuis plus de trente ans. Telle était la durée du copyright américain en 1928 (*Free culture, op. cit.*, p. 24).

330. - En ce sens, V.-L. Bénabou (prés.) et D. Botteghi (rapp.), *La mise à disposition ouverte des œuvres de l'esprit*, rapport CSPLA, juin 2007, n° 60 : « [...] le droit exclusif ne s'entend pas uniquement comme un droit d'interdire, mais constitue également un droit d'autoriser, qui peut le cas échéant s'exercer à titre gratuit si telle est la volonté de l'auteur ». Le rapport rappelle l'existence de l'article L. 122-7-1 CPI : « L'auteur est libre de mettre ses œuvres gratuitement à la disposition du public, sous réserve des droits des éventuels coauteurs et de ceux des tiers ainsi que dans le respect des conventions qu'il a conclues ».

331. - M. Clément-Fontaine, *L'œuvre libre*, préf. M. vivant, éd. Larcier, 2014, n° 104.

332. - S. Broca et P. Eynaud, « Biens communs et outils numériques : le cas des logiciels libres », *Juris associations*, 2014, n° 501, p. 33.

*must pass on to the recipients the same freedoms that you received. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights*³³³.

Un très grand nombre de modèles de contrats ont été conçus dans cet esprit depuis, dans le seul domaine des logiciels d'abord, puis en matière d'œuvres de l'esprit plus généralement³³⁴. Madame Clément-Fontaine a tenté d'ordonner cette diversité autour d'une notion unitaire de « licences libres », définies comme « (...) les licences par lesquelles l'auteur autorise la copie, la modification et la diffusion de l'œuvre modifiée ou non, de façon concurrente, sans transférer les droits d'auteur qui y sont attachés et sans que l'utilisateur puisse réduire ces libertés tant à l'égard de l'œuvre originelle que de ses dérivés »³³⁵.

241. Les palettes de licences — Comme leur nom l'indique, les licences *Creative commons* — qui doivent beaucoup à M. Lessig - prétendent elles aussi contribuer à la constitution de « communs » culturels³³⁶. Le titulaire du droit d'auteur est invité à répondre à deux questions³³⁷. En fonction des réponses, de petits pictogrammes seront apposés à côté de l'œuvre, accompagnés d'un lien vers un résumé du contenu de la licence accessible aux non-juristes. La simplicité de mise en œuvre a assuré à ces contrats un important succès populaire³³⁸.

À la première question, « souhaitez-vous autoriser le partage des adaptations de votre œuvre ? », il est possible de répondre par « oui », « non », « oui sous condition de partage dans les mêmes conditions ». À la deuxième question, « autorisez-vous les utilisations commerciales de votre œuvre », il est simplement possible de répondre par l'affirmative ou la négative.

Si l'utilisateur refuse les œuvres dérivées, le site lui précise que la licence en résultant ne sera pas considérée comme relevant de la « Free culture ». S'il les autorise purement et simplement, le label « Free culture » lui sera décerné, mais il ne s'agira pas d'une licence libre au sens où l'entendait Madame Clément-Fontaine. En effet, la licence ne sera pas « virale » : l'auteur de l'œuvre dérivée pourra faire valoir son monopole dans des conditions classiques, ce que ne permettrait absolument pas la GPL, par exemple.

333. - GNU General Public License, version 3, 29 juin 2007 : <http://www.gnu.org/licenses/gpl.html>.

334. - V. not. l'excellent tableau de synthèse qui permet à M. Clément-Fontaine de proposer une comparaison détaillée des licences GPL, CECILL, Berkeley Software Foundation, European Union Public Licence, Creative commons BY-SA et Licence Art Libre : *op. cit.*, tableau 1 en annexe, p. 488 s.

335. - M. Clément-Fontaine, *op. cit.*, n° 756.

336. - L. Lessig, *Free culture*, *op. cit.*, spéc. p. 282 s., « Rebuilding free culture : one idea ».

337. - <https://creativecommons.org/choose/>.

338. - L. Lessig, *Free culture*, *op. cit.*, p. 282 : «

242. **Un problème contingent : la clause d'usage non commercial** - L'auteur qui choisirait, pour sa licence *Creative Commons*, d'interdire les utilisations commerciales de son œuvre, se verrait par ailleurs lui aussi préciser : « ceci n'est pas une licence Free culture ». Dans l'esprit du grand public, les licences libres sont parfois conçues comme les véhicules d'usages exclusivement non marchands. Cela n'est pas exact. En effet :

*Les personnes qui viennent participer à l'évolution de l'œuvre vont partager la jouissance de cette œuvre et peuvent en outre, comme tout un chacun, utiliser l'œuvre à des fins scientifiques, culturelles, mais aussi à des fins mercantiles. Ce cercle vertueux contribue au développement des œuvres libres. Or, la clause non commerciale va à l'encontre de ce dynamisme dans la mesure où seule la création initiale entre dans la sphère économique tandis que toutes les contributions ultérieures en sont exclues. La clause non commerciale emporte le risque par conséquent de restreindre pour ne pas dire éteindre la motivation des utilisateurs à participer à son développement de sorte que l'œuvre demeurerait en son état initial*³³⁹.

De manière plus préoccupante encore, la clause produit des effets juridiques incertains, car elle est particulièrement difficile à interpréter³⁴⁰. Un récent contentieux américain en fournit une illustration³⁴¹. Une association à but non lucratif, *Great Minds*, proposait des contenus à visée éducative sous licence CC « Paternité – Pas d'usage commercial – Partage à l'identique »³⁴². Plutôt que d'imprimer elle-même les fascicules, une école qui souhaitait les utiliser au bénéfice de ses élèves avait eu recours à un service d'impression à la demande proposé par la FedEx. *Great Minds* décida d'attaquer le reprographe, soutenant qu'il avait violé la licence en se faisant rémunérer pour réaliser des copies de l'œuvre. Le juge n'a pas suivi ce raisonnement :

*(...) La licence emploie le terme « Vous », défini comme « l'individu ou l'entité exerçant les droits conférés » et l'autorise à « reproduire ou partager le contenu, en tout ou partie, seulement à des fins non-commerciales ». Dans cette affaire, les entités qui exercent les « droits conférés » sont les écoles, et non FedEx, et il n'est pas contesté que les écoles reproduisent ou partagent les contenus dans un but non-commercial. Comme ce sont bien les écoles qui exercent les droits conférés par la licence, on ne peut considérer que FedEx a fait un usage commercial des contenus en étant employé par les écoles (...)*³⁴³.

339. - M. Clément-Fontaine, *op. cit.*, p. 363.

340. - .-L. Bénabou (prés.) et D. Bottegghi (rapp.), *La mise à disposition ouverte des œuvres de l'esprit*, rapport préc., n° 88 s ; M. Clément-Fontaine, « La clause non commerciale des licences ouvertes : sécurité juridique, libre concurrence et valorisation », *AJCA*, 2015, p. 164. V. les multiples exemples discutés par E. Prodromou sur le Framablog : <https://framablog.org/2012/10/15/non-commercial-creative-commons/>.

341. - D. Kravets, « Odd lawquit fails to ding FedEx for allowing copies of CC-licensed material », article *arstechnica.com* du 27 février 2017 ; L. Maurel, « Quand la clause Non-Commercial des licences Creative Commons passe en justice », article *scinfolex.com* du 8 mars 2017. La *motion to dismiss* du défendeur Fedex peut être consultée ici : <https://creativecommons.org/wp-content/uploads/2016/08/2016-08-24-Defendant-Fedex-Motion-to-Dismiss.pdf>.

342. - <https://creativecommons.org/licenses/by-nc-sa/4.0/legalcode>.

343. - La décision est consultable ici :

Ce problème peut être qualifié de « contingent », dans la mesure où il ne concerne que certaines variantes des licences *Creatives Commons*, qui ne sont pas véritablement des licences libres : celles qui prohibent les utilisations commerciales. En revanche, l'ensemble des licences véritablement libres se heurte à de sérieux problèmes de compatibilité avec le droit d'auteur français.

243. Des problèmes structurels - Des difficultés plus profondes affectent l'utilisation des licences libres en droit français. Comme l'explique Madame Clément-Fontaine, elles résultent des principes qui sont au fondement même de la conception française de la propriété littéraire et artistique :

[Une licence libre] heurte les règles d'ordre public du droit d'auteur, notamment les règles de protection relatives à l'interprétation stricte des cessions et à l'inaliénabilité de la protection de l'intégrité de l'œuvre. Or, ces règles ont été conçues selon une approche individualiste de la création qui serait le résultat d'une seule personne et de ce fait intangible. Les œuvres libres sont, au contraire, des œuvres évolutives au gré de l'intervention des contributeurs. L'auteur n'est donc pas solitaire, mais crée avec d'autres personnes dans un rapport d'égalité³⁴⁴.

D'abord, l'auteur évoque le principe d'interprétation stricte des cessions de droit d'auteur. En effet, après avoir exposé que le droit de représentation et le droit de reproduction doivent être cédés distinctement, le Code de la propriété intellectuelle ajoute : « Lorsqu'un contrat comporte cession totale de l'un des deux droits visés au présent article, la portée en est limitée aux modes d'exploitation prévus au contrat »³⁴⁵. Or, Madame Clément-Fontaine estime qu'il est impossible, en pratique, d'anticiper tous les usages et toutes les finalités d'exploitation que les licences libres entendent permettre, et par conséquent d'en établir une liste dans le contrat³⁴⁶. La règle n'a pas été pensée pour mettre des droits à disposition du public entier, afin qu'il en fasse tout ce que lui dicte son imagination.

Ensuite, lorsque la question des usages transformatifs a été abordée, il a été exposé que retenir une conception trop puissante des droits moraux de l'auteur, en particulier du droit au respect de l'intégrité de l'œuvre, serait problématique.³⁴⁷ Ce droit pourrait être brandi pour s'opposer à la constitution d'un écosystème créatif autour de l'œuvre d'origine, au prétexte d'une trahison de son esprit. La question avait été soulevée dans un contexte où les usages transformatifs se développaient sans l'autorisation de l'auteur, par exemple en vertu d'une exception à son droit de propriété : il

<https://arstechnica.com/wp-content/uploads/2017/02/greatmindsdecision.pdf>. Traduction en français proposée par L. Maurel, « Quand la clause Non-Commercial... », art. préc.

344. - M. Clément-Fontaine, *op. cit.*, n° 756.

345. - Art. L. 122-7 CPI.

346. - M. Clément-Fontaine, *op. cit.*, n° 201.

347. - V. *supra*, n° 226.

était alors logique d'envisager qu'il use des instruments mis à sa disposition pour empêcher des usages de son œuvre qui lui déplairaient dans leur principe même. Cette difficulté ne devrait pas se présenter, pourrait-on croire, lorsque le même auteur accorde une licence libre et s'inscrit donc spontanément dans une démarche d'utilisation collective de sa création : ne renonce-t-il pas nécessairement à user du droit moral en contradiction avec sa démarche ? Ce serait oublier qu'aux termes de la loi, ce droit est « inaliénable »³⁴⁸. Une interprétation modérée du droit au respect de l'intégrité de l'œuvre aplanit cependant une partie des problèmes³⁴⁹.

L'une et l'autre des deux difficultés présentées appellent une même remarque quelque peu rassurante. En effet, « [...] en dépit d'un éventuel risque de contradiction entre les termes contractuels des licences et la législation nationale, le contentieux est presque inexistant, ce qui s'explique essentiellement par la cohérence de l'engagement pris par ceux qui ont recours aux licences libres et qui entendent adhérer à cette philosophie »³⁵⁰.

Faut-il cependant se contenter de relever cette absence de contentieux, et s'en satisfaire ? Ce serait passer à côté du sens général de la démonstration de Madame Clément-Fontaine. Elle propose qu'à côté d'une propriété classique, individualiste et verticale, soit reconnue l'existence d'une forme nouvelle de propriété, non pas concurrente, mais alternative. Il est alors question de « communs » ou de « domaine public consenti », qui appellent des règles de gestion horizontales par de larges groupes, les communautés³⁵¹. La loi doit alors intervenir pour fixer un régime adapté. Cela n'empêcherait pas le droit français et européen de conserver un noyau de valeurs impératives, mais de laisser pour le surplus à la volonté le soin d'opter pour l'application de corps de règles radicalement différents. Une analogie à caractère strictement pédagogique peut être proposée avec les régimes matrimoniaux, qui offrent la possibilité aux individus de choisir des statuts nettement différents, en leur imposant toutefois un cœur de règles baptisé « régime primaire ».

II - Le droit sur les copies d'œuvres

244. Propriété contre propriété - Une représentation courante des rapports entre numérique et droit d'auteur voudrait que le premier soit à l'origine d'un mouvement clair et univoque

348. - Art. L. 121-1 CPI, al. 3.

349. - V. *supra*, n°226.

350. - V.-L. Bénabou (présidente) et F. Langrognet (rapporteur), *Rapport de la mission du CSPLA sur les « œuvres transformatives »*, préc., p. 39.

351. - M. Clément-Fontaine, *op. cit.*, partie II : « le partage de l'avoir ou une propriété collective ». *Adde*, du même auteur, « L'œuvre numérique : un élément iconoclaste en droit de la propriété » in *Les biens numériques*, éd. Ceprisca, 2015, p. 183, spéc. section 2 : « l'œuvre numérique et les communs » et 3 « pour un partage pacifique ».

d'affaiblissement du second. Ce cliché a déjà été énoncé, notamment lors de la présentation des mesures techniques de protection (MTP), qui constituent de puissantes sentinelles numériques au service de la propriété littéraire et artistique³⁵². Dans certaines situations, la perte de contrôle des utilités de l'œuvre par les ayants droit, qui pouvait légitimement inquiéter, laisse aujourd'hui la place à un excès en sens inverse : ceux qui croient acheter des exemplaires numériques de l'œuvre se trouvent investis de droits qu'ils peuvent juger insuffisants.

L'une des explications à ce phénomène tient peut-être à la disparition des supports sur lesquels les œuvres étaient auparavant distribuées. À la propriété de l'auteur sur l'œuvre, le consommateur de produits culturels était en mesure d'opposer la propriété d'un exemplaire physique. La maîtrise de fait qu'il exerçait sur cette chose tangible était en quelque sorte constatée par le droit, qui lui reconnaissait implicitement un certain nombre de prérogatives, par exemple la possibilité de procéder à la revente d'occasion de son vinyle, de son CD-ROM ou de son tirage papier de l'œuvre.

L'emploi de technologies numériques de distribution des œuvres entraîne la disparition progressive de ces supports (A). La CJUE a cru devoir résister aux conséquences juridiques de ce mouvement par le jeu d'une fiction juridique : la reconnaissance des copies immatérielles de l'œuvre (B).

A - La disparition progressive des supports

245. **L'exemple du jeu vidéo** - Le marché des consoles de jeu constitue une illustration frappante du mouvement de disparition des supports. Cet exemple n'est pas choisi au hasard : la réaction de la CJUE, qui sera évoquée plus loin, s'est produite sur le terrain du droit des logiciels, famille d'objets intellectuels à laquelle les jeux vidéo appartiennent³⁵³.

Le marché des consoles est essentiellement aux mains d'un oligopole formé par Sony et ses Playstation, Microsoft et ses Xbox, Nintendo et ses Wii U. Mi-2013, une nouvelle génération de machines doit être présentée au public³⁵⁴. C'est Microsoft qui prend l'initiative, en présentant les principales caractéristiques de la future Xbox One dans le cadre de l'*Electronic Entertainment Expo* (E3) à Los Angeles. Ces annonces provoquent, au sein de la communauté des joueurs, une stupeur qui se transforme rapidement en indignation³⁵⁵. On apprend en effet que la console refusera de

352. - V.supra, n°233.

353. - Les développements qui vont suivre sont largement issus de notre étude « Le logiciel dématérialisé », in *Les biens numériques*, éd. Ceprisca, 2015, p. 149.

354. - La *Wii U* était déjà sortie, peu de temps auparavant. Il restait donc à annoncer les machines de Sony et de Microsoft.

355. - V. par ex. J. Marin, « La nouvelle console de Microsoft sous le feu des critiques », article *lemonde.fr* du

fonctionner si elle ne bénéficie pas d'un accès permanent — tout du moins quotidien — à Internet³⁵⁶. Ensuite, le prêt gratuit de jeu à un ami sera fortement restreint, voire empêché³⁵⁷. Enfin et surtout, la revente d'occasion ne sera possible que par l'intermédiaire d'un marchand agréé par Microsoft, et moyennant le prélèvement d'une commission³⁵⁸. Ces trois caractéristiques formaient un tout cohérent. L'accès permanent à Internet n'était pas exigé dans le seul intérêt de l'utilisateur. Il ne visait pas exclusivement à irriguer sa console de fonctionnalités multijoueurs ou de l'accès permanent à un réseau d'amis. Il s'agissait surtout de vérifier, à chaque instant, que la console exécutait des logiciels dans la stricte mesure des autorisations accordées par Microsoft. Lancer un jeu prêté par son grand frère ? Il aurait fallu entrer préalablement les codes d'accès Microsoft du prêteur - ce qui l'aurait empêché de jouer simultanément, sur sa propre console, à un autre jeu. Utiliser un DVD-ROM légalement acheté par un premier joueur, mais revendu directement à un second joueur ? Impossible.

Sony, qui devait présenter sa Playstation 4 un peu plus tard, a habilement réagi au tollé suscité par son concurrent. Parodiant et moquant les méthodes de Microsoft, Sony a diffusé une vidéo intitulée : *Official Playstation used game instructional video*³⁵⁹. On y voit deux individus, dont le premier tient dans les mains un boîtier plastique renfermant un DVD. Il déclare : « Voici comment on prête un jeu sur la Playstation 4 »³⁶⁰. Il se tourne vers son comparse et lui tend la boîte. Son collègue saisit l'objet et lui dit « merci ! » : fin de la vidéo. Lors de sa conférence de presse, le président de Sony Computer Entertainment pour l'Amérique a précisé sa philosophie : « Lorsque les joueurs achètent un disque pour la Playstation 4, **ils ont le droit d'utiliser cette copie du jeu, de la vendre à quelqu'un, de la prêter à un ami ou de la conserver indéfiniment** »³⁶¹. Les concepts juridiques mobilisés par ce discours doivent être relevés. L'utilisateur du logiciel a « acheté » une « copie » du jeu, sur laquelle il doit exercer, en toute liberté, des prérogatives qui évoquent largement celles d'un propriétaire. Ce droit réel s'exerce d'une manière concrète, palpable, par une emprise matérielle sur une chose corporelle, le « disque » du jeu. Dans la vidéo

10 juin 2013.

356. - « Xbox One does require internet connection, can't play offline forever », article du 21 mai 2013 sur www.kotaku.com.

357. - « Xbox One : le grand cafouillage de Microsoft », article du 23 mai 2013 consultable sur <http://obsession.nouvelobs.com/high-tech/20130523.OBS0448/xbox-one-le-grand-cafouillage-de-microsoft.html>.

358. - J. Marin, art. préc.

359. - Cette vidéo est toujours consultable sur le compte *YouTube* officiel de la *Playstation*.

360. - « *This is how you share a game on PS4* ».

361. - « *When a gamer buys a PS4 disc, they have the rights to use that copy of the game, they can trade in the game at retail, sell it to another person, lend it to a friend or keep it forever* ». Souligné par nous. Pour une retranscription de ces propos : <http://www.scpr.org/blogs/newmedia/2013/06/11/13951/video-e3-sony-launches-playstation-4-while-trollin/>.

humoristique, cette chose se transmet par tradition réelle, de la main à la main. L'idée sous-jacente est parfaitement claire : il y a quelque chose de naturel dans ce geste. Symétriquement, le joueur peut et doit ressentir un malaise lorsque le concurrent essaie de lui retirer cette prérogative. Le porte-parole de Sony tenant ce discours a été acclamé par le public³⁶². *Microsoft* a été contraint à une marche arrière rapide et quelque peu humiliante³⁶³ : la console fonctionnera finalement même non connectée à Internet ; il sera possible de prêter ses jeux ; il sera possible de les revendre.

Encore faut-il apporter une précision fondamentale. Les seuls jeux dont les utilisateurs disposent librement sont ceux vendus sur des supports physiques : aussi bien Sony que *Microsoft* ont totalement exclu la mise en place d'un marché de l'occasion pour les programmes dématérialisés acquis par la voie du téléchargement légal³⁶⁴. Impossible, par ailleurs, de prêter à un proche un programme obtenu ainsi. La version physique et la version dématérialisée du logiciel, souvent vendues au même prix, font donc l'objet d'un traitement très différent. Pourtant, l'utilisateur exploitera, dans les deux cas, des fichiers identiques. Simplement, dans un cas, ces fichiers lui auront été transmis par l'intermédiaire d'une galette de plastique gravée ; dans l'autre, par l'intermédiaire d'un flux d'information transitant par des fils de cuivre ou des fibres optiques.

La disparition du support physique de commercialisation de l'œuvre produit donc, à l'évidence, des conséquences sur le terrain des prérogatives juridiques reconnues par les grandes firmes du jeu vidéo à leurs clients. Comment l'expliquer ?

246. Propriété de l'œuvre et propriété du support - Les rapports complexes entre l'œuvre et son support fascinaient déjà les Romains. Dans les *Institutes*, on trouve la question suivante : « Lorsqu'on a peint sur la toile d'autrui, quelques-uns pensent que la toile est l'accessoire de la peinture ; d'autres pensent que la peinture, quelle qu'elle soit, est l'accessoire de la toile : le premier sentiment nous paraît préférable . Ne serait-il pas en effet ridicule qu'un ouvrage de peinture d'Appelle ou de Parrhasius fût regardé comme l'accessoire d'une toile d'un vil prix ? »³⁶⁵. L'approche est assez fruste, puisqu'il s'agit d'établir, entre l'artiste et le propriétaire du support, qui est le dominant et qui est le dominé. Les critères utilisés — valeur économique du support, prestige de l'artiste — laissent craindre une solution au cas par cas. La solution des droits modernes est tout autre : il s'agit de superposer sur une même chose deux « propriétés », en tout cas deux ensembles de prérogatives dont les objets sont différents et compatibles. Aux termes de l'article L. 111-3 al.

362. - *Ibid.*

363. - *Microsoft* contraint de faire marche arrière sur sa Xbox One, article www.lemonde.fr du 19 juin 2013.

364. - *Ibid.*

365. - *Les Institutes de l'Empereur Justinien*, trad. M. Hulot, citées par C. Caron, *op. cit.*, n° 26.

1er du CPI, « La propriété incorporelle définie par l'article L. 111-1 est indépendante de la propriété de l'objet matériel ». Il s'agit alors davantage de protéger l'auteur que l'amateur d'art. Avant que le sculpteur ne vende sa statue, en effet, aucune difficulté n'est susceptible de surgir. Une fois qu'il l'a vendue, en revanche, c'est l'acheteur qui se trouve, *a priori*, en nette position de force. Propriétaire de la chose, il pourrait se prévaloir de l'article 544 du Code civil pour en disposer selon son bon plaisir. La distinction entre œuvre et support permet à l'auteur d'invoquer un lien invisible et permanent, qui le relie à tout objet incorporant son art, afin de freiner, tempérer, modérer les prérogatives du propriétaire du support. Ainsi, ce n'est pas parce que l'on achète un tableau que l'on acquiert le droit de le reproduire sur des cartes postales puis de les vendre : cette prérogative continuera d'appartenir au titulaire du droit d'auteur, et à lui seul³⁶⁶. Quoique cette idée paraisse aujourd'hui relativement simple, les principes fondamentaux de la propriété intellectuelle ayant suffisamment infusé dans l'esprit collectif, elle exige un certain degré de raffinement du système juridique, et n'a pas toujours été admise par le passé³⁶⁷.

Les exemples précédents étaient articulés autour de supports de création, c'est-à-dire de choses sur lesquelles le pouvoir créateur de l'auteur s'était directement exercé : manuscrit original ou toile de maître par exemple³⁶⁸. S'agissant des logiciels, la vente porte uniquement sur des supports de commercialisation : l'œuvre originale est dupliquée et s'incarne dans de simples exemplaires, des copies³⁶⁹. Ce sont ces copies qui sont vendues. La tension existant entre les droits de l'auteur et ceux du propriétaire du support s'amenuise. Que le propriétaire d'une simple copie exerce son droit d'en disposer en la mutilant ou en la dégradant, cela est parfaitement indifférent à l'auteur, alors que le même comportement en présence d'un support de création aurait éventuellement porté atteinte à ses prérogatives extrapatrimoniales — le droit au respect de l'œuvre — et patrimoniales – son droit

366. - Art. L. 113-2 CPI : l'acquéreur du support « [...] n'est investi du fait de cette acquisition, d'aucun des droits prévus par le présent code ».

367. - La Cour de cassation avait ainsi tranché en sens inverse il y a longtemps « [...] le droit de reproduire le tableau par la gravure doit être compris au nombre des droits et facultés que transmet l'acquéreur d'une vente sans réserve [...] » (Ch. Réunies, 27 mai 1842).

368. - « Si la doctrine reconnaît majoritairement que l'œuvre doit se comprendre comme une forme perceptible aux sens, elle ne répond pas à la question de la réalisation du passage entre l'idée et la forme. Cette mutation ne peut en effet être permise que par l'intervention d'un corps ou d'un véhicule qui porte l'expression de l'œuvre. L'œuvre de l'esprit a besoin d'un instrument assurant sa perception. Un auteur ne peut en effet faire sortir l'œuvre de son imaginaire qu'en utilisant un vecteur capable d'extérioriser l'œuvre afin de la rendre perceptible par autrui. C'est cet instrument que l'on dénomme support de création » (L. Breuker, « Le support de création et le support de commercialisation de l'œuvre », *CCE*, n° 1, janv. 2003, chron. 2).

369. - « Si la réalisation d'une œuvre nécessite la présence d'un support de création, l'œuvre ne reste pas attachée à cette première empreinte physique. L'œuvre de l'esprit est en effet une chose incorporelle dotée d'un don d'ubiquité qui lui permet d'être présente à la fois en différents lieux. C'est cette faculté que le législateur entend protéger en accordant un monopole d'exploitation à l'auteur. Or, la mise en œuvre de ce monopole d'exploitation nécessite un outil assurant la communication de l'œuvre. Le support de commercialisation se présente alors comme l'instrument assurant la dissociation de l'œuvre d'avec son support de création » (*ibid.*).

de reproduction. Les droits réels sont cantonnés, maintenus presque naturellement dans un juste équilibre, dans la mesure où ils s'exercent sur un simple avatar, sur une incarnation de l'œuvre parmi des milliers d'autres. Cela ne signifie pas que l'auteur exerce son emprise uniquement sur l'original, tandis que l'acheteur l'exerce sur la copie. Non : le support, fût-il un simple support de commercialisation, reste toujours soumis au droit d'auteur. Ainsi, être propriétaire d'un exemplaire sur CD-ROM d'un logiciel n'autorisera jamais à le dupliquer et à revendre les clones ainsi créés. Mais le petit Yalta des prérogatives sur l'œuvre s'opère avec une relative aisance. Le droit du propriétaire du support de commercialisation est fort - sans être menaçant. Considérons l'exemple concret de la vente d'occasion sur les marchés aux puces.

Sur les étals d'un vide-grenier, on trouvera souvent des dizaines de jeux vidéo, anciens ou récents, sous forme de boîtiers contenant des CD ou DVD-ROM. Voici un individu qui paie quelques euros, et repart avec l'une de ces galettes de plastique sous le bras. Avons-nous assisté à la conclusion d'un contrat de vente ? La question est discutée³⁷⁰. L'opération n'a pas pu se limiter à cela, car pour donner l'ordre à sa console de salon ou à son ordinateur personnel d'exécuter le jeu d'instructions contenu sur le disque, l'utilisateur doit y avoir été autorisé par le titulaire des droits sur le logiciel. Pour ce faire, l'acquéreur initial du logiciel avait dû accepter d'entrer dans les liens d'un contrat que la pratique nomme souvent « contrat de licence ». Ce terme ne doit pas être compris dans un sens étroit, qui renverrait au droit des brevets — or, on l'a vu, le logiciel relève du droit d'auteur — mais dans le sens large et originel du mot *licencia* : c'est une autorisation³⁷¹. Elle emporte concession du droit de transférer le logiciel dans la mémoire de la machine et de l'y mettre en œuvre. Pour que la vente du support d'un jeu vidéo sur les marchés aux puces ait un quelconque intérêt, il faut donc considérer que l'acheteur de ce support se voit également céder les droits contractuels permettant son exploitation. De manière invisible, la « licence » a donc circulé, comme collée au support. Les parties, sans même en avoir conscience, ont conclu un accord global qui semble avoir emporté cession de droits réels, mais aussi substitution au sein d'une position contractuelle liant l'utilisateur du logiciel à l'éditeur. Le contrat de licence est en quelque sorte réifié par adhésion au support, en vertu du principe selon lequel l'accessoire suit le principal.

370. - V. not. *Lamy Droit du numérique, op. cit.*, n° 740, paragraphe intitulé : « La tentative de qualifier comme vente le contrat de fourniture d'un logiciel standard ».

371. - *Ibid.*, n° 741. La convention est parfois considérée comme *sui generis* (par ex. A. Hollande et X. Linant de Bellefonds, *Pratique du droit de l'informatique et de l'internet*, Editions Delmas, 6e éd., 2008, n° 503). Nous avons pourtant critiqué le recours à une qualification ad hoc dans le cadre des textes relatifs au droit de rétractation. Mais c'est une chose de dire que le contrat de fourniture de progiciel n'est, dans une analyse rigoureuse, identique à aucun autre contrat existant. C'en est une autre de refuser de le classer dans les grandes catégories et de n'y voir ni la fourniture d'un bien, ni celle d'un service.

247. **Une marche forcée vers « l'âge de l'accès »** - Mais voici que disparaissent les exemplaires matériels. Le retournement est spectaculaire. Nous avons décrit des titulaires du droit d'auteur courant après les propriétaires de supports (de création, mais aussi de commercialisation), en brandissant des constructions intellectuelles sophistiquées pour faire contrepoint à la toute-puissance apparente de leur droit de propriété. Aujourd'hui, l'utilisateur de logiciel est nu. Sans support à brandir, il manque de points d'accroche pour justifier de ses prérogatives. Que reste-t-il dans son patrimoine ? Des droits personnels, des droits de créance nés du contrat de licence, qui ne constituent plus l'accessoire, mais le principal. Ainsi un auteur écrit-il : « Fournir un accès à une œuvre, sans en transférer la propriété du support, relève de la prestation de services. C'est mettre l'œuvre à la disposition d'un utilisateur, pendant un certain temps ou dans certaines limites. Accorder à l'utilisateur une relative jouissance de l'œuvre peut pareillement être qualifié de prestation de services [...] »³⁷². Un autre auteur estime, dans le même ordre d'idées, que l'on est passé d'un commerce de copies à « un commerce de droits » ou même à un « commerce de positions normatives »³⁷³ : on n'achète plus qu'une position contractuelle.

Ces tendances sont parfaitement cohérentes avec les théories de l'essayiste américain Jeremy Rifkin. Selon lui, nous sommes entrés dans une ère de « l'accès » : d'une économie basée sur le droit de propriété, le marché et le contrat de vente, nous serions en train de passer à une logique globale d'accès, de réseau et de prestations de services³⁷⁴.

Il n'est pas exclu qu'une partie des consommateurs de produits culturels accepte bien volontiers de basculer dans cette logique, et de troquer la propriété d'une dvdthèque pour un abonnement Netflix. Il faut toutefois remarquer, d'une part, qu'il subsiste sans doute une partie de la population attachée à la propriété d'exemplaires d'œuvres de l'esprit, d'autre part que le commerce d'accès précaires à des biens culturels numériques fait un emploi constant et trompeur du champ lexical de la vente - c'est-à-dire qu'il prétend transférer une propriété. L'exemple des magasins d'application

372. - S. Dussolier, *Droit d'auteur et protection des œuvres dans l'univers numérique*, préf. A. Lucas, avant-propos Y. Pouillet, 2007, n° 509.

373. - J. Bing, cité par S. Dussolier, *loc. cit.*

374. - J. Rifkin, *The Age of Access : The New Culture of Hypercapitalism, Where All of Life Is a Paid-For Experience*, New York, Jeremy P. Tarcher/Putnam, 2000. Extrait de l'article de présentation publié par l'auteur dans la revue *Resurgences*, n° 207, en 2001 : « *In the new era, markets are making way for networks, and ownership is steadily being replaced by access. Companies and consumers are beginning to abandon the central reality of modern economic life—the market exchange of property between buyers and sellers. Instead, suppliers hold on to property in the new economy and lease, rent or charge an admission fee, subscription of membership dues for its use. The exchange of property between buyers and sellers—the most important feature of the modern market system—gives way to access between servers and clients operating in a network relationship. Many companies no longer sell things to one another but rather pool and share their collective resources creating vast supplier-user networks.* ». Pour une analyse juridique de ce phénomène : C. Castets-Renard, « Des biens aux services numériques : de l'ère de la propriété à l'âge de l'accès », in *Les biens numériques*, éd. Ceprisca, 2015, p. 203.

est frappant. Lorsqu'il est question d'acquérir un programme, le bouton est toujours libellé « acheter »³⁷⁵. Dans l'esprit de l'utilisateur, dès lors, même en l'absence de support tangible, il s'agit d'acquérir des droits définitifs, des droits de propriété, et non pas une autorisation contractuelle précaire, limitée dans le temps ou dans l'usage qu'il est permis d'en faire, et incessible. D'ailleurs, ce vocabulaire ne se retrouve pas uniquement sur les pages destinées au grand public. Même les conditions générales cultivent parfois une surprenante ambiguïté. Ainsi peut-on lire chez *Google Play* : « Lorsque vous **achetez** du Contenu (défini comme des fichiers de données, **des applications**, du texte écrit, un logiciel d'appareil mobile, de la musique, des fichiers audio ou d'autres sons, des photographies, des vidéos ou d'autres images) sur *Google Play*, vous **l'achèterez** : (a) directement auprès de la société *Google Commerce Limited* (une “**Vente** directe”) [...] »³⁷⁶. L'internaute aurait tort d'arrêter là sa lecture, car un peu plus loin il découvrira : « Vous ne pouvez pas vendre, louer, redistribuer, diffuser, transmettre, communiquer, modifier, concéder ou céder tout Contenu ou vos droits relatifs au Contenu à tout tiers sans autorisation [...] »³⁷⁷. Sur *Steam*, l'interface destinée au grand public use et abuse des mots « achat » et « vente ». En revanche, les conditions générales sont d'emblée très claires : « Les Contenus et Services sont concédés sous licence, et non vendus. Votre licence ne vous confère aucun droit ni titre de propriété sur les Contenus et Services. Pour utiliser les Contenus et Services, vous devez être en possession d'un Compte *Steam* et vous pouvez être tenu d'exécuter le client *Steam* et d'être connecté à Internet pendant toute la durée d'utilisation »³⁷⁸. S'il s'agit de dire que le client ne devient pas propriétaire de l'œuvre, c'est une évidence que personne n'aurait songé à contester. Il s'agit bien de lui refuser la propriété d'une copie. Ce faisant, on lui retire notamment la faculté de céder ses droits d'utiliser un exemplaire de l'œuvre.

La CJUE a tenté de s'opposer à ce mouvement, en adoptant un arrêt audacieux et controversé.

B - Le maintien artificiel des copies

248. **L'épuisement du droit de distribution** - L'entreprise américaine Oracle développe des logiciels à usage professionnel, notamment dans le domaine des bases de données. Elle les distribue aussi bien sous forme physique que sous forme dématérialisée, selon la préférence de ses clients.

375. - Le lecteur pourra en faire l'expérience sur *Google Play*, sur l'*App Store*, sur *Steam*...

376. - Conditions d'utilisation du 17 novembre 2014, consultables sur https://play.google.com/intl/fr_fr/about/play-terms.html, partie 2 « Fourniture de *Google Play* ».

377. - *Ibid.*, partie 6 « Droits et restrictions ».

378. - Conditions générales *Steam* du 15 mars 2015, consultables sur http://store.steampowered.com/subscriber_agreement/french/.

85% des utilisateurs optent déjà pour une livraison du logiciel par téléchargement : cela ne fait aucun doute, nous sommes en train de vivre les dernières années du CD-ROM³⁷⁹. Le problème est venu de ce qu'une entreprise allemande, Usedsoft GMBH, avait pris l'initiative d'organiser un marché secondaire des licences pour les logiciels Oracle. Certains clients, en effet, n'avaient plus l'usage des programmes achetés quelques années plus tôt au prix fort. D'autres n'avaient qu'un usage partiel des licences : chacune d'entre elles autorisait l'utilisation du logiciel sur 25 postes au maximum. Dès lors, exécuter les instructions sur 26 ordinateurs rendait nécessaire l'acquisition de deux licences ; Usedsoft proposait alors de « revendre » à un autre professionnel les droits non utilisés, correspondant dans notre exemple à 24 postes de travail. Une fois en possession de la licence de seconde main, l'entreprise se connectait aux serveurs d'Oracle, y téléchargeait le logiciel et l'exécutait sur ses machines.

Oracle saisit la justice allemande aux fins d'interdire à Usedsoft la poursuite de ses activités. Elle faisait notamment valoir qu'au sein du contrat de licence, figurait la clause suivante, intitulée « Droit concédé » : « Le paiement des services vous donne un droit d'utilisation à durée indéterminée, non exclusif, **non cessible** et gratuit, réservé à un usage professionnel interne, pour tous les produits et services qu'Oracle développe et met à votre disposition sur le fondement du présent contrat »³⁸⁰.

La principale question posée par ce litige était celle de savoir si le droit de distribution d'Oracle était épuisé³⁸¹. En effet, la directive du 23 avril 2009 « concernant la protection juridique des programmes d'ordinateur » énumère les droits exclusifs de l'auteur d'un logiciel : droit de reproduction, d'adaptation, d'arrangement... et droit de distribution des copies du programme³⁸². Mais une restriction importante est aussitôt apportée au dernier de ces droits : « La **première vente d'une copie d'un programme** d'ordinateur dans la Communauté par le titulaire du droit ou avec son consentement **épuise le droit de distribution** de cette copie dans la Communauté [...] »³⁸³. Cette théorie de l'épuisement du droit est présentée tantôt comme d'origine allemande³⁸⁴, tantôt

379. - Le chiffre est cité par la Cour dans les premières lignes de sa décision.

380. - Souligné par nous.

381. - Par contrecoup, une autre question fondamentale était de savoir si l'entreprise ayant « acheté » le logiciel d'occasion était un « acquéreur légitime » au sens de l'article 5.1 de la directive de 2009.

382. - Art. 4, 1.

383. - Art. 4, 2. Souligné par nous.

384. - M. Vivant et J.-M. Bruguière, *op. cit.*, n° 493 : « [la CJUE] a imaginé de puiser dans le “fonds juridique” allemand pour en tirer cette théorie de l'épuisement du droit d'où il résulte que chaque droit de propriété intellectuelle a “un objet spécifique” et qu'une fois celui-ci réalisé, “épuisé”, le titulaire des droits ne peut plus rien réclamer [...] ». La théorie de l'épuisement est ainsi susceptible de s'appliquer à d'autres prérogatives de l'auteur que le droit de distribution.

comme d'inspiration américaine³⁸⁵. Elle limite les prérogatives de l'auteur au bénéfice de la libre circulation des marchandises au sein de l'Union : passée la première vente, le destin de la copie du logiciel doit définitivement lui échapper.

Lorsqu'*Oracle* distribue ses logiciels par la voie du téléchargement, le contrat peut-il être analysé comme une « première vente » ? L'objet de cette vente est-il une « copie de programme » ? Ces difficultés d'interprétation d'un texte européen devaient être tranchées, au niveau de l'Union, par la CJUE : aussi le *Bundesgerichtshof* allemand, dernière juridiction saisie dans l'ordre interne, lui posa-t-il plusieurs questions préjudicielles.

249. La fiction des copies immatérielles - La Cour relève que la directive ne renvoie pas aux droits nationaux pour la définition de ce qu'est une « vente », et en déduit qu'il s'agit d'une notion autonome du droit de l'Union³⁸⁶. S'étant dès lors affranchie de toute contrainte, la CJUE définit très librement la vente comme « une convention par laquelle une personne cède, moyennant le paiement d'un prix, à une autre personne ses droits de propriété sur un bien corporel ou incorporel lui appartenant »³⁸⁷. *Oracle* affirmait qu'il y avait conclusion d'un contrat de licence, puis mise à disposition gratuite de fichiers sur son serveur, mais qu'il n'y avait là aucun transfert de propriété d'aucune sorte³⁸⁸. À cette analyse fragmentée, la Cour répond par une approche globalisante : « il convient de relever que le téléchargement d'une copie d'un programme d'ordinateur et la conclusion d'un contrat de licence d'utilisation se rapportant à celle-ci forment un tout indivisible. En effet, le téléchargement d'une copie d'un programme d'ordinateur est dépourvu d'utilité si ladite copie ne peut pas être utilisée par son détenteur. Ces deux opérations doivent dès lors être examinées dans leur ensemble aux fins de leur qualification juridique »³⁸⁹. Examiner isolément le contrat dit « de licence » n'aurait pas permis d'aboutir à la qualification de vente. La CJUE a fourbi ses armes : une définition de la vente spécialement forgée pour l'occasion ; une approche bien particulière de la qualification qui, sous prétexte de considérer l'économie générale de l'opération ou l'ensemble contractuel dans son entier, se focalise sur le tout et délaisse les parties. On rencontre alors le centre de gravité de l'arrêt : « le client d'*Oracle*, qui télécharge la copie du programme d'ordinateur concerné et qui conclut avec cette société un contrat de licence d'utilisation portant sur ladite copie, reçoit, moyennant le paiement d'un prix, un droit d'utilisation de cette copie **d'une**

385. - Par ex. P. Gaudrat, obs. précitées sur l'arrêt *Usedsoft*, n°1. Il s'agit cette fois-ci non pas de la notion générale d'épuisement du droit (cf. note précédente), mais spécifiquement de l'épuisement du droit de distribution, présenté comme inspiré de la « *first sale doctrine* » des pays de copyright.

386. - §40.

387. - §42.

388. - §43.

389. - §44.

durée illimitée. La mise à la disposition par Oracle d'une copie de son programme d'ordinateur et la conclusion d'un contrat de licence d'utilisation y afférente visent ainsi à rendre ladite copie utilisable par ses clients, **de manière permanente**, moyennant le paiement d'un prix destiné à permettre au titulaire du droit d'auteur d'obtenir une rémunération correspondant à la valeur économique de la copie de l'œuvre dont il est propriétaire »³⁹⁰. Pour la Cour, on peut bel et bien parler de copie immatérielle d'un logiciel. Surtout, cette copie est susceptible de faire l'objet d'un droit réel et plus spécifiquement d'un droit de propriété de la part du client. Ce sera le cas lorsque les droits d'utilisation du programme auront été octroyés à titre définitif, permanent. On en déduit, *a contrario*, qu'un droit temporaire d'utilisation du logiciel relèverait du monde des droits personnels, des droits de créance, et naîtrait par exemple d'un simple bail.

La CJUE va encore plus loin. Pour protéger les acquéreurs de logiciels téléchargés, elle n'utilise pas de concept propre à l'immatériel. Bien au contraire, elle affirme qu'il existe une véritable égalité fonctionnelle et juridique entre les deux types de véhicules que constituent le CD et le flux d'informations à travers un réseau : « **il est indifférent**, dans une situation telle que celle en cause au principal, que la copie du programme d'ordinateur ait été mise à la disposition du client par le titulaire du droit concerné au moyen d'un téléchargement à partir du site Internet de ce dernier ou au moyen d'un support matériel tel qu'un CD-ROM ou un DVD. [...] il doit être considéré que **ces deux opérations impliquent également**, dans le cas d'une mise à la disposition d'une copie du programme d'ordinateur concerné au moyen d'un support matériel tel qu'un CD-ROM ou un DVD, **le transfert du droit de propriété de ladite copie** »³⁹¹.

250. **Éviter l'éviction des biens par les contrats** - L'arrêt Usedsoft a parfois fait l'objet de vives critiques³⁹². Il faut reconnaître qu'il sollicite fortement les concepts.

Initialement, la théorie de l'épuisement du droit de distribution visait les seuls exemplaires matériels, et n'était qu'un instrument au service de la libre circulation des marchandises. Mais elle semble prendre, depuis quelques années, une ampleur nouvelle. Sans même viser l'arrêt Usedsoft, des auteurs écrivaient ainsi : « [...] la reconnaissance de l'épuisement du droit — fût-il limité en notre matière au droit de distribution — comme un “standard” européen, visé dans les directives,

390. - §45. Souligné par nous.

391. - §47. Souligné par nous.

392. - En particulier P. Gaudrat, obs. préc., n° 25 et s., use d'expressions sévères : « [...] Aussi pour ne pas affronter son incohérence, la Cour se lance-t-elle dans un syllogisme parasite, du même acabit, qui, au lieu d'établir la qualification défailante, se contente de nier qu'il puisse en exister une autre, comme le soutenait Oracle ! [...] Pour dissimuler leur embarras et faire passer pour incohérent l'argument auquel ils avaient peine à répondre, les juges communautaires donnent libre cours à leur fantaisie [...]. Admirable dénouement de la pensée qui conduit à faire passer une affirmation gratuite pour la conclusion d'un raisonnement ! [...] ».

voire les règlements [...] en étend sensiblement la portée. L'épuisement n'est plus seulement le moyen d'assurer la libre circulation intracommunautaire. Il devient une composante intrinsèque des droits. Autrement dit, la théorie de l'épuisement interdit certes à un titulaire de droits intellectuels de contrôler la circulation du bien en cause entre Berlin et Paris, mais aussi et tout autant entre Toulouse et Rouen »³⁹³. Conçu à l'origine comme un simple instrument de mise en œuvre du marché commun, l'épuisement du droit de distribution est déformé par la Cour, afin qu'il produise des conséquences sur la substance même des droits des utilisateurs de logiciels, y compris dans un cadre purement national. Cette théorie est, de surcroît, associée à la notion de copie immatérielle, qui est avant tout une fiction juridique, une vue de l'esprit, destinée à autoriser un raisonnement sur le terrain du droit des biens, là où il n'y aurait sans cela que des contrats. Assurément, la Cour donne à des instruments juridiques un sens nouveau, joue avec les concepts, et s'expose — certainement en toute conscience — à de multiples critiques techniques. Mais n'est-ce pas toujours le prix à payer lorsque l'on rend une décision fondatrice, qui fait profondément évoluer le droit ? Quelles alternatives, plus respectueuses des cadres existants, la doctrine a-t-elle proposées pour éviter que les grandes sociétés de la net-économie ne finissent par fixer unilatéralement les règles du jeu dans leurs contrats d'adhésion ? L'arrêt *Usedsoft* est une décision courageuse, qui invite les pouvoirs normatifs et les auteurs à s'interroger sur l'avenir du logiciel dématérialisé. Au-delà, même, c'est l'ensemble de la distribution d'œuvres dématérialisées qui pourrait faire l'objet de raisonnements similaires : si c'est un droit spécial du logiciel qui est appliqué en l'espèce, une fois le raisonnement ramené à une épure, on voit mal comment éviter de poser des questions identiques à propos des livres, des films ou de la musique³⁹⁴.

Il ne faut cependant pas en surestimer la portée pratique.

251. L'effet limité de l'arrêt *Usedsoft* - Les auteurs critiques à l'encontre de la CJUE devraient néanmoins en convenir : il devenait de plus en plus difficile de soutenir qu'un régime juridique différent devait être appliqué aux copies matérielles et aux copies immatérielles de logiciels. Dès 2004, le fonctionnement de la plateforme de vente de jeux vidéo Steam montrait que cette distinction deviendrait sans issue. Les acheteurs du vidéo *Half-Life 2*, lorsqu'ils rentraient chez eux avec leur CD-ROM, avaient la surprise de ne pas pouvoir commencer à jouer immédiatement. Ils avaient l'obligation de se connecter à la plateforme-forme Steam et d'y créer un compte personnel. Il fallait alors fournir la clé CD unique imprimée à l'intérieur de la jaquette du jeu. Dès cet instant, le logiciel se liait irrévocablement au compte utilisateur. Il était alors possible de procéder à son

393. - M. Vivant et J.-M. Bruguière, *op. cit.*, n° 493.

394. - En ce sens, V. not. les obs. préc. de C. Le Stanc et celles d'E. Treppoz.

installation soit par lecture optique des données figurant sur la galette de plastique, soit par téléchargement sur le site de l'éditeur, de manière parfaitement indifférente. Dans les deux cas, il est impossible de détacher l'exemplaire du jeu du compte personnel, et donc de le prêter, de le vendre ou de le donner à un autre utilisateur.

La distinction entre copies matérielles et immatérielles du logiciel est donc en train de disparaître, pour laisser place à des règles indifférenciées principalement gouvernées par les mesures techniques de protection. Dire que Steam ou Apple empêche le prêt des objets culturels acquis auprès d'eux est en réalité inexact. Tous deux proposent un système de « partage familial » ou amical³⁹⁵. La marque à la pomme propose ainsi : « Avec le Partage familial, six personnes de votre foyer peuvent partager les achats effectués par les uns et les autres sur l'iTunes Store, l'iBooks Store et l'App Store. En toute simplicité et sans avoir à partager leurs comptes ». D'où vient ce chiffre de « six » ? Qu'est-ce qu'un « foyer » au sens de cette entreprise ? Combien de temps ces règles resteront-elles valables ? C'est le contrat qui en décide, et les MTP qui sont son bras armé. Le droit réel sur le support est remplacé par une « normativité embarquée », issue d'un pur contrat d'adhésion³⁹⁶.

Ainsi, la montée en puissance des MTP semble soutenir la décision *Usedsoft*, puisqu'elle procède à un nivellement par le bas des droits des utilisateurs de copies matérielles, en les alignant sur ceux des copies immatérielles. Mais ces mêmes MTP constituent le talon d'Achille de la décision :

*[...] si l'arrêt de la Cour n'interdit pas [le commerce de logiciels de seconde main], elle n'oblige pas les éditeurs à le faciliter, et rien ne semble devoir empêcher ces éditeurs de mettre en place les protections techniques destinées à le restreindre. On sait, par ailleurs, par exemple pour les applications de téléphone mobiles, ou de jeux vidéo, que leur usage, lié à des comptes utilisateurs, ne peut en être désolidarisé [...]*³⁹⁷.

Aujourd'hui, un logiciel spécialisé — voire le système d'exploitation lui-même, par exemple iOS — sera chargé de s'assurer que la « copie » d'œuvre à laquelle un utilisateur cherche à accéder sur sa machine lui est bien attribuée dans le registre officiel tenu par un serveur distant : il s'instaure un dialogue entre *trusted systems*³⁹⁸. Qui a déjà tenté de revendre d'occasion une application achetée pour son téléphone intelligent ? L'idée ne vient même plus à l'esprit de l'utilisateur, accoutumé à

395. - Steam : <http://store.steampowered.com/promotion/familysharing?l=french>. Apple : <https://www.apple.com/fr/ios/whats-new/family-sharing/>.

396. - Sur le sens que nous donnons à « système normatif embarqué », V. supra, n°233.

397. - C. Le Stanc, obs. sur l'arrêt *Usedsoft* précité.

398. - C'est la logique des *trusted system*, sur lesquels V. not. L. Lessig, *Code V2*, op. cit., p. 178 et s. ainsi que S. Dusollier, *Droit d'auteur et protection des œuvres dans l'univers numérique*, op. cit.

une architecture pensée pour que cela soit simplement impossible. Il n'est plus titulaire d'aucun droit réel. La définition même d'un tel droit voudrait d'ailleurs qu'il soit « immédiat », c'est-à-dire que l'utilité de la chose puisse être retirée sans qu'il soit besoin de transiter par un intermédiaire³⁹⁹. Or, la conception même des *trusted systems* implique que cette situation ne sera produira presque plus jamais dans l'univers numérique. Restent des comptes utilisateurs, qui sont autant de patrimoines de carton-pâte, dont on est bien en peine de définir le contenu. Si ce ne sont pas des droits réels, il s'agit alors de créances. Mais si c'est un droit de durée illimitée qui a été acquis, que devient la prohibition des engagements perpétuels ? Quel sort réserver à ces créances, dans le cas d'une faillite du « vendeur » du bien culturel, qui empêcherait les utilisateurs de continuer à accéder à leurs copies d'œuvres ? Les richesses numériques sont-elles transmissibles à cause de mort⁴⁰⁰ ? Aucune de ces questions ne reçoit, à l'heure actuelle, de réponse véritablement satisfaisante.

252. **Pistes de réforme** - Deux grandes orientations peuvent être identifiées : l'une serait libérale, l'autre plus interventionniste.

Il est possible d'opter pour une approche libérale, c'est-à-dire que l'on abandonnerait au marché la détermination des prérogatives des utilisateurs sur les produits. L'étendue du pouvoir de disposition de l'acquéreur sur sa copie serait une composante de l'offre au même titre que la qualité du contenu ou son prix. Rien n'interdit d'imaginer, d'ailleurs, qu'un logiciel ou plus largement un contenu culturel soit proposé en deux versions, à des prix différents, l'une incessible, l'autre susceptible d'être prêtée ou vendue. En faveur de cette autorégulation, certains pourraient citer l'exemple de la guerre des consoles de nouvelle génération, décrite en ouverture de cette étude. Microsoft cherchait à réduire les pouvoirs des acheteurs de logiciels. Sony a proposé une alternative plus généreuse, ce qui lui a offert un avantage concurrentiel tel que Microsoft a dû faire marche arrière. C'est en quelque sorte au public qu'il revient de voter, avec son portefeuille⁴⁰¹. Mais même

399. - Le droit réel peut être défini comme « un droit qui porte directement et immédiatement sur une chose individuellement déterminée, dont il permet de retirer, sans emprunter l'intermédiaire d'une personne obligée, l'utilité légale totale ou partielle et qui exige de tous un respect égal, mais purement passif » : L. Rigaud, *Le droit réel. Histoire et théories. Son origine institutionnelle*, thèse Toulouse, 1912, p. 116, cité par W. Dross, *Droit des biens*, op. cit., note 45 p. 121.

400. - Rappelons que la loi prévoit depuis peu dans quelles conditions les données personnelles du défunt peuvent être transmises à ses héritiers à cause de mort : art. 40-1 de la loi 78-17 précitée, V.supra, n°117. Le texte évoque certes la « [...] **communication des biens numériques** ou des données s'apparentant à des souvenirs de famille » (souligné par nous). Mais si l'on visait par là les copies immatérielles d'œuvres, ce qui est douteux, il faudrait s'interroger sur la place de cette solution dans un texte visant la dévolution des données, qui ne sont pas des biens, mais des prolongements de la personne. Il est assez ironique de constater que le principe de « dévolution unitaire des patrimoines tangible et numérique » a été invoqué, au cours des travaux parlementaires, pour justifier des solutions en matière de données personnelles — qui ne relèvent pas du patrimoine — mais que rien n'a été décidé s'agissant de la postérité à donner à la jurisprudence *Usedsoft* - qui pose quant à elle véritablement cette question.

401. - Ainsi, en matière de jeux vidéo pour ordinateur, plusieurs plateformes déjà citées arrivent à concurrencer

dans ce modèle, les pouvoirs publics ne doivent pas rester totalement passifs. Ils doivent au minimum s'assurer que les conditions d'une concurrence libre et non faussée sont réunies. Le public est parfois séduit par une machine qui l'oblige ensuite à recourir à un unique fournisseur de contenus — Apple et son iPhone en constituent un excellent exemple — excluant le jeu normal de la concurrence. La question de la propriété des terminaux sera d'ailleurs examinée, en tant que telle, un peu plus loin⁴⁰². Les géants du numérique à l'échelle mondiale sont peu nombreux, et le risque que des quasi-monopoles ne se constituent, à l'échelle d'un type de contenu culturel particulier, n'est pas nul. Ensuite, même si l'offre est variée, la concurrence ne fonctionne que si le public est suffisamment informé sur l'étendue de ses droits. Le rôle des autorités consiste alors, au minimum, à vérifier que la transparence est assurée. La contradiction permanente, que nous avons relevée, entre le champ lexical de la vente dans les documents marketing, et la stipulation de licences restrictives dans des documents juridiques qui ne sont lus par personne, est à cet égard inquiétante. Ces restrictions devraient être signalées de manière beaucoup plus explicite⁴⁰³.

Une autre approche, plus interventionniste, est envisageable. Le législateur — national ou européen — interviendrait de manière autoritaire pour obliger les grands du numérique à octroyer certaines prérogatives à leurs clients. La CJUE pourra difficilement remplir un rôle identique à elle seule. Si elle était saisie par un utilisateur souhaitant que le juge enjoigne à Apple, par exemple, de lui donner les moyens techniques de revendre une application pour iPhone, que ferait-elle ? Considérerait-elle que c'est une conséquence logique de la décision *Usedsoft* ? Il est difficile de le dire⁴⁰⁴. Pour remettre en cause les strates de mesures techniques de protection accumulées, et surtout des systèmes fondamentalement conçus pour exclure de telles transactions entre utilisateurs, il faudrait toute l'autorité de la loi. Trois directions principales se dessineraient alors. La première direction consiste à traiter les contenus numériques comme des objets juridiques à part entière, sans chercher à les rattacher à des catégories ou à des régimes préexistants. C'est la voie du *sui generis*, qui présente elle aussi ses inconvénients. Déconnecter une question du droit commun – en l'occurrence du droit d'auteur, du droit des biens ou droit des contrats communs, c'est la priver de sève, c'est l'assécher. Dès lors que la réglementation spéciale n'est pas exhaustive, en effet, les solutions viennent à manquer. Le droit commun, lui, n'est jamais silencieux. La deuxième direction

Steam en proposant des produits « sans DRM » : *Good Old Games* ou *Humble Bundle* par exemple.

402. - V.infra, n° 253 s.

403. - Comp. TGI Nanterre, 15 déc. 2006, *UFC Que Choisir c/ Sté Sony France et Sté Sony UK : Propriétés intellectuelles*, 200, n° 23, p. 222, obs. J.-M. Bruguière. Cette société proposait au téléchargement de la musique qui ne pouvait être lue que sur des baladeurs numériques de la même marque. Le fait de ne pas l'indiquer explicitement a été considéré par le tribunal comme constitutif de délit de tromperie.

404. - C. Le Stanc, obs. préc., ne le pense pas.

envisageable serait celle du droit des contrats. On pourrait notamment imaginer que les clauses empêchant l'acquéreur du logiciel de disposer de son droit d'utilisation ou de sa licence soient déclarées abusives. La question du champ d'application *ratione personae* se poserait alors : il serait envisageable de protéger uniquement les non-professionnels ou consommateurs, en considérant que les professionnels sont suffisamment aptes à jauger et négocier les contrats ; il serait possible, au contraire, de placer l'ensemble des acquéreurs de logiciels sous l'égide d'une législation impérative. La troisième direction consisterait à solliciter le droit des biens. Suivant la voie tracée par la CJUE, en se fondant sur l'analyse économique du droit et sur la notion d'équivalence fonctionnelle, il s'agirait de promouvoir le concept de copie immatérielle d'un logiciel – ou d'une chanson, ou d'un film, ou d'un livre numérique. Agir ainsi, ce serait perpétuer pour l'avenir le souvenir du support physique et son régime, quitte à adapter les concepts. Comme si le fantôme ne pouvait jamais vraiment oublier son corps de chair... Peut-être faut-il éviter de basculer totalement dans « l'âge de l'accès ». Peut-être que le concept de propriété, dont la puissance est non seulement juridique, mais aussi symbolique, politique, ne doit pas devenir l'apanage des sociétés de distribution des contenus culturels, mais rester aussi aux mains du public. La propriété modérerait la propriété.

C'est précisément cette idée qu'il faut décliner, pour finir, en l'appliquant aux terminaux plutôt qu'aux seuls contenus.

Section 3 - Les terminaux

253. **Les systèmes « fermés »** – Nous sommes en 1984. Dans quelques minutes, la société Apple annoncera le lancement du premier Macintosh, lors d'une *keynote* à grand spectacle comme Steve Jobs en avait le secret. Malheureusement, un problème technique affecte le module vocal de la machine de démonstration, qui risque de ne pas pouvoir lancer au monde, ainsi qu'il était prévu : « Hello, I'm Macintosh ». Un ingénieur reçoit l'ordre de le réparer de toute urgence. Malheureusement, il a oublié chez lui les outils spéciaux qui permettent d'ouvrir la machine. À son assistante, qui s'étonne qu'on ne puisse pas ouvrir le Mac avec des tournevis classiques, Jobs répond qu'il entendait créer un système fermé « *end-to-end* », aussi bien du point de vue matériel que logiciel. Les réglages auxquels le client peut avoir accès doivent être en nombre limité, et les plus superficiels possible. L'acheteur entre dans un univers où il accepte de déléguer à la compagnie la moindre parcelle de contrôle, pour bénéficier d'une « expérience utilisateur » présentée comme la plus simple et la plus ergonomique possible⁴⁰⁵.

405. - La scène est relatée dans le film *Steve Jobs* de Danny Boyle, sorti au cinéma en France en février 2016. L'auteur remercie vivement Lionel Maurel, qui lui a suggéré cette illustration en même temps que de nombreuses

Aujourd'hui encore, la société Apple pousse à son paroxysme cette logique de verrouillage – mais elle n'est plus la seule. Une telle démarche ne va-t-elle pas à l'encontre du droit de propriété de l'utilisateur sur son terminal ?

254. **Un droit à réparer ?** - D'un point de vue matériel, nombreux sont les modèles d'iMac auxquels le propriétaire ne pourra même pas ajouter une barrette de mémoire RAM sans passer par le service après-vente. La grande majorité des téléphones intelligents, quelle que soit leur marque, ne peut faire l'objet d'une réparation simple ni d'un remplacement de la batterie.

D'aucuns pourraient mettre en avant la complexité croissante de ces systèmes pour abdiquer par avance tout droit des utilisateurs à « ouvrir leur capot ». La *Repair association* américaine attire cependant l'attention sur des stratégies délibérées visant à empêcher les propriétaires de s'assurer un contrôle matériel de leurs machines : utilisation de mesures physiques pour les en empêcher — les fameuses vis d'Apple, incompatibles avec les tournevis courants, existent toujours — et absence de diffusion des éléments techniques élémentaires permettant de comprendre comment la machine est assemblée, et à quoi correspondent les différents composants⁴⁰⁶. Elle demande la généralisation, à tous les domaines y compris le matériel électronique et informatique, de lois telles que le *Motor Vehicle Owner's Right to Repair Act* du New Jersey⁴⁰⁷. Ce texte dispose notamment :

*(...) a manufacturer of motor vehicles sold in the State shall make available for purchase by owners of motor vehicles manufactured by such manufacturers and by independent repair facilities the same diagnostic and repair information, including repair technical updates, that such manufacturer makes available to its dealers through the manufacturer's internet-based diagnostic and repair information system or other electronically accessible manufacturer's repair information system (...)*⁴⁰⁸.

De telles dispositions ont plusieurs objectifs. Elles augmentent le pouvoir d'achat des consommateurs, en stimulant la concurrence dans les prestations de fourniture de pièces de rechange et de réparation. Mais elles ont aussi un effet environnemental : le coût de la réparation s'abaisse, notamment parce qu'il est possible d'y procéder soi-même. Il n'est plus nécessaire de jeter puis de remplacer la chose abîmée.

255. **Le verrouillage logiciel** – Pour importantes qu'elles soient, les difficultés à réparer ne sont probablement pas les aspects les plus redoutables des systèmes dits « fermés ». Dans un rapport de mai 2017, voué à être suivi d'approfondissements ultérieurs, l'ARCEP donne une première mesure

références qui ont nourri les réflexions présentées dans cette section.

406. - V. le site repair.org.

407. - *Motor Vehicle Owner's Right to Repair Act* , N° 4336, 9 septembre 2013, consultable ici : http://www.njleg.state.nj.us/2012/Bills/A4500/4336_11.PDF.

408. - Art. 3, a. de la loi précitée.

de « l'influence sur l'ouverture de l'Internet » qu'ont les terminaux⁴⁰⁹. L'Autorité estime à juste titre que le droit d'accéder à un Internet neutre, ouvert et innovant » reconnu par un règlement européen dépend non seulement de la neutralité du réseau et de la loyauté des plateformes, questions déjà abordées, mais encore de la manière dont sont conçus les « terminaux »⁴¹⁰. Sous ce concept, tombent notamment les appareils mobiles de communication (téléphones intelligents et tablettes), les ordinateurs, les box des FAI, les consoles de jeux vidéo, les téléviseurs et autres objets connectés⁴¹¹. À l'intérieur de ces appareils, la couche logicielle (comprenant notamment le système d'exploitation, mais aussi les programmes spécialisés) procède à de multiples restrictions des usages possibles de l'appareil, parfois sans que l'utilisateur en ait véritablement conscience. Quelques exemples seront choisis parmi les nombreux qui sont développés par l'ARCEP.

256. L'obsolescence du système d'exploitation – Après quelques années, les ordinateurs ou téléphones intelligents ne bénéficient plus d'une mise à jour de leur principal logiciel. Il y a de bonnes, mais aussi de mauvaises raisons à ce phénomène : « Les fournisseurs de systèmes d'exploitation peuvent vouloir limiter le nombre de versions du système d'exploitation en circulation, par exemple pour augmenter le niveau de sécurité de la plateforme, pour limiter leurs coûts, ou pour inciter les utilisateurs à basculer vers leurs produits les plus récents »⁴¹². Ce sont d'abord les applications qui posent problème : au fur et à mesure, elles cesseront d'être disponibles pour la version du système d'exploitation (ou *OS* pour *Operating System*) considérée comme trop ancienne⁴¹³. Puis, au bout d'un moment, les failles de sécurité de l'OS lui-même n'étant plus corrigées, il deviendra dangereux de continuer à utiliser la machine. La possibilité d'y installer un système d'exploitation sous licence libre, parfois moins gourmand en ressources que la dernière version de l'OS propriétaire, et maintenu à jour par la communauté, permettra de poursuivre

409. - ARCEP, *Équipements terminaux. Analyse de leur influence sur l'ouverture de l'Internet*, 30 mai 2017 : https://www.arcep.fr/uploads/tx_gspublication/etude-place-terminaux-ouverture-internet-300517.pdf.

410. - « Le 30 avril 2016, le règlement européen 2015/2120 sur l'internet ouvert entrain en vigueur. Il consacrait un droit pour les utilisateurs finals d'accéder à un internet neutre, ouvert et innovant et d'y fournir des contenus (...) Constatant que les questions posées par les terminaux restent encore mal identifiées, l'Arcep estime qu'il est essentiel d'analyser la capacité des utilisateurs, quel que soit leur terminal, d'accéder et de contribuer aux différents contenus et applications de l'Internet » (rapport préc., p. 2).

411. - Rapport préc., p. 12.

412. - Rapport préc., p. 15.

413. - Il y a une explication technique à ce phénomène : « Afin de stimuler l'extinction des versions les plus anciennes, le développeur du système d'exploitation peut, à la faveur d'une mise à jour, décider de ne plus donner accès à des *API* (*Applications Programming Interface*) préalablement mises à disposition des développeurs d'applications. Il en résulte qu'une application disponible sur une version ancienne d'un système d'exploitation peut disparaître lorsque cette version n'est plus maintenue, dès lors que son fournisseur n'est pas en mesure de réaliser les investissements nécessaires pour recoder les fonctions de base. Ainsi, des utilisateurs n'ayant pas téléchargé les versions les plus récentes d'un système d'exploitation peuvent perdre l'accès à certaines de leurs applications, ou être privés des mises à jour de certaines applications » (rapport préc., p. 15).

l'utilisation d'un ordinateur. Cette possibilité est empêchée sur les téléphones intelligents par l'emploi de mesures techniques de protection. Ainsi, une machine encore parfaitement fonctionnelle sur le plan matériel finira dans un tiroir ou une décharge.

257. Le recours obligatoire à un unique magasin d'applications - Plus grave encore : chez certains fournisseurs, l'achat du terminal impose de passer par le magasin d'applications de la marque pour y installer de nouvelles fonctionnalités. C'est le cas sur les téléphones Apple. Les téléphones sous système Android peuvent recourir à des magasins d'applications alternatifs, mais encore l'utilisateur doit-il le savoir et décider d'en faire usage. Or, celui qui contrôle un magasin d'applications incontournable dispose, vis-à-vis de sa clientèle, de leviers à la fois commerciaux et intellectuels d'une puissance inouïe.

Parmi les milliers de logiciels candidats à l'achat ou à l'installation gratuite – accompagnée de publicités ou d'achats intégrés, c'est le magasin qui décide qui sera mis en avant, ce qui lui donne le pouvoir de vie et de mort sur les développeurs qui s'adressent à lui⁴¹⁴. Le vendeur des terminaux pourra même imposer ses propres applications préinstallées dans certains secteurs, ce qui lui confèrera un avantage décisif sur les applications tierces⁴¹⁵. Ensuite, puisque le magasin occupe une situation de monopole ou de quasi-monopole, les développeurs qui veulent s'adresser à ses clients doivent lui verser une commission, dont le montant pourra d'autant moins être négocié qu'il n'existe pas d'alternative pour toucher le public ayant acheté les terminaux de cette marque.

Par ailleurs, des enjeux dépassant de loin les seules questions économiques peuvent être identifiés. Comme le résume pudiquement l'ARCEP, « L'accès à certains contenus jugés sensibles peut, sans que cela ne résulte du seul respect de la loi, être limité par un magasin d'applications contrôlé par un acteur soucieux de préserver son image de marque »⁴¹⁶. Un fabricant de terminaux imposant son magasin d'applications s'est ainsi distingué par son refus de l'application d'un caricaturiste américain, lauréat peu de temps après du prix Pulitzer⁴¹⁷. Un développeur commentait l'affaire ainsi : « (...) Ils nous traitent comme des enfants à qui on dit fais pas ci, fais pas ça.

414. - Rapport préc., p. 17 : « De manière générale, les politiques de référencement et de mise en avant des contenus dans les magasins d'applications sont peu transparentes. (...) il est possible que certaines limites résultent en réalité d'enjeux de concurrence : les magasins d'applications peuvent privilégier des services verticalement intégrés en entravant le bon fonctionnement des applications concurrentes (...). L'entrave ne passerait pas nécessairement par un blocage réel des applications visées : elle pourrait prendre la forme d'une durée d'homologation allongée pour certaines applications [...] ».

415. - L'ARCEP relève toutefois que « (...) la pré-installation d'applications essentielles peut répondre aux attentes d'utilisateurs finals qui souhaitent pouvoir utiliser leur équipement dès la première prise en main » (*Loc. cit.*).

416. - *Loc. cit.*

417. - O. Chicheportiche, « Censure sur l'AppStore : Apple s'emmêle les pinceaux avec un Prix Pulitzer », article *zdnet.fr* du 19 avril 2010.

Internet est un monde libre et l'idée qu'un groupe californien décide du bon goût pour ses utilisateurs est un peu gênante »⁴¹⁸. Récemment, la même marque a retiré les applications du New York Times de son magasin d'applications chinois⁴¹⁹.

En somme, le contrôle du magasin d'applications est susceptible d'entraîner une mainmise sur les portefeuilles et sur les esprits.

Aux divers problèmes qui viennent d'être présentés, il faut ajouter ceux décrits plus tôt dans l'étude. Ainsi l'impossibilité de revendre ou d'offrir à une autre personne un exemplaire d'une œuvre de l'esprit — film, musique, logiciel... — résulte d'un modèle contractuel, doublé de mesures de protection, qui a été mis en place par les magasins dominants⁴²⁰. S'il était possible de recourir à des systèmes d'exploitation et à des magasins alternatifs, rien n'empêcherait de concevoir d'autres équilibres. En certains points, la question de la propriété des terminaux et celle de la propriété des copies immatérielles de contenus se rejoignent donc.

Voyons à présent comme les droits américain puis européen ont réagi face à ces différents enjeux.

258. Aux USA : un « droit au jailbreak » - Une campagne « *Jailbreaking is not a crime* » a été menée aux États-Unis par l'*Electronic Frontier Foundation* (EFF)⁴²¹. Le mot « *jailbreak* » — évasion— désigne le fait de contourner les mesures techniques de protection d'un terminal afin d'y installer un système d'exploitation librement choisi par l'utilisateur. Il est couramment utilisé pour les téléphones, mais peut en réalité désigner tout appareil sur lequel le choix est en principe interdit par le constructeur, comme une console de jeux vidéo. Le discours favorable à la légalité de cette pratique se fonde explicitement sur le droit de propriété dont peut se prévaloir l'acheteur de la machine :

*You bought it. You own it. Tell the Copyright Office: let me install whatever software I want on my phone, tablet, or video game system*⁴²².

Aux USA comme en France, le contournement de mesures techniques de protection est en principe interdit⁴²³. Mais au sein du *Digital Millenium Copyright Act*, une procédure a été mise en place permettant d'examiner, tous les trois ans, si des contournements précis méritent d'être

418. - Art. préc., citant C. McCathieNeville, responsable des standards pour Opera Software.

419. - K. Banner et W. Sui-Lee, « Apple removes New York Times apps from its store in China », article *nytimes.com* du 4 janvier 2017.

420. - V. supra, n° 251.

421. - <https://act.eff.org/action/jailbreaking-is-not-a-crime>.

422. - <https://www.jailbreakingisnotacrime.org/>.

423. - Sur le droit français en la matière, V. supra, n°231.

autorisés, parce qu'il serait constaté que les MTP empêchent des usages légitimes et non contrefaisants de matériaux protégés⁴²⁴. L'EFF s'en est saisie, avec succès, pour obtenir en 2010 un « droit au *jailbreak* » sur les téléphones intelligents :

*(...) On balance, the Register concludes that when one jailbreaks a smartphone in order to make the operating system on that phone interoperable with an independently created application that has not been approved by the maker of the smartphone or the maker of its operating system, the modifications that are made purely for the purpose of such interoperability are fair uses. Case law and Congressional enactments reflect a judgment that interoperability is favored. The Register also finds that designating a class of works that would permit jailbreaking for purposes of interoperability will not adversely affect the market for or value of the copyrighted works to the copyright owner*⁴²⁵.

Ce système d'autorisation est temporaire, et la demande doit être renouvelée tous les deux ou trois ans. En 2012, l'autorisation de contourner les MTP a été renouvelée pour les téléphones, mais refusée pour les consoles de jeux. En 2015, l'autorisation a été renouvelée à nouveau pour les téléphones⁴²⁶.

Une tentative d'aborder ces problèmes de manière plus large, et par la voie législative, a été initiée en 2014 avec un texte intitulé *Your Own Device Act*. Elle a échoué, mais le texte a été réintroduit il y a peu devant le Congrès, de manière conjointe, par un représentant républicain et un démocrate⁴²⁷.

259. En Europe : l'arrêt Nintendo de la CJUE – En droit de l'Union, il n'existe pas d'équivalent du mécanisme américain d'autorisation temporaire de contournement des mesures de

424. - 17 U.S. Code § 1201 - Circumvention of copyright protection systems :
A) No person shall circumvent a technological measure that effectively controls access to a work protected under this title (...).
(B) The prohibition contained in subparagraph (A) shall not apply to persons who are users of a copyrighted work which is in a particular class of works, if such persons are, or are likely to be in the succeeding 3-year period, adversely affected by virtue of such prohibition in their ability to make noninfringing uses of that particular class of works under this title, as determined under subparagraph (C).
(C) (...) during each succeeding 3-year period, the Librarian of Congress, upon the recommendation of the Register of Copyrights, who shall consult with the Assistant Secretary for Communications and Information of the Department of Commerce and report and comment on his or her views in making such recommendation, shall make the determination in a rulemaking proceeding for purposes of subparagraph (B) of whether persons who are users of a copyrighted work are, or are likely to be in the succeeding 3-year period, adversely affected by the prohibition under subparagraph (A) in their ability to make noninfringing uses under this title of a particular class of copyrighted works.

425. - Library of Congress, Copyright office, 37 CFR Part 201, *Exemption to prohibition on circumvention of copyright protection systems for access control technologies*, Federal Register vol. 75, n° 143, 27 juillet 2010 : <https://www.gpo.gov/fdsys/pkg/FR-2010-07-27/pdf/2010-18339.pdf>.

426. - Les différentes décisions sont consultables à l'adresse : <https://www.copyright.gov/1201/>.

427. - K. Sheehan, « YODA, the Bill That Would Let You Own (and Sell) Your Devices, Is Re-Introduced in Congress », article *eff.org* du 7 février 2017.

protection. Mais d'autres fondements peuvent être invoqués par les partisans du *jailbreak*, comme le rappelle un arrêt *Nintendo* de la Cour de Justice⁴²⁸.

L'affaire concernait les consoles Wii et DS vendues par cette entreprise. Les machines comprennent un système de reconnaissance associé à un code crypté, qui vise officiellement à empêcher l'utilisation de copies illégales de jeux vidéo. Cependant, une société dénommée PC Box commercialisait ces machines, dans une version comprenant un système d'exploitation altéré de sorte à désactiver les MTP. Selon Nintendo, l'objectif était de favoriser l'utilisation de copies contrefaites des œuvres dont elle détient les droits. Selon PC Box, « la finalité réelle poursuivie par les entreprises Nintendo est d'empêcher l'utilisation d'un "software" indépendant, qui ne constitue pas une copie illégale de jeux vidéo, mais qui est destiné à permettre la lecture sur les consoles de fichiers MP3, de films et de vidéos, afin d'exploiter pleinement ces consoles »⁴²⁹.

La Cour constate que rien, dans la directive de 2001 sur l'harmonisation du droit d'auteur, n'oblige à protéger les œuvres en se contentant de MTP figurant exclusivement sur le support de commercialisation : il est licite d'intégrer la protection, pour partie, dans la machine destinée à interagir avec le support⁴³⁰. En raisonnant par analogie, on peut considérer que rien n'interdit non plus que le siège de la protection d'applications ou de contenus multimédias se situe pour partie dans un terminal téléphonique.

Une fois le droit des MTP considéré comme applicable, la principale question est de savoir si les mesures en cause sont proportionnées. Un considérant de la directive précisait en effet : « Une telle protection juridique doit respecter le principe de proportionnalité et ne doit pas interdire les dispositifs ou activités qui ont, sur le plan commercial, un objet ou une utilisation autre que le contournement de la protection technique »⁴³¹. C'est là que se situe le cœur de la décision :

*(...) aux fins de l'examen du but desdits dispositifs, produits ou composants, la preuve de l'usage que font effectivement de ceux-ci les tiers va être, en fonction des circonstances en cause, particulièrement pertinente. La juridiction de renvoi peut, notamment, examiner la fréquence avec laquelle les appareils de PC Box sont effectivement utilisés pour que des copies non autorisées de jeux Nintendo et sous licence Nintendo puissent être utilisées sur des consoles Nintendo ainsi que la fréquence avec laquelle ces appareils sont utilisés à des fins qui ne violent pas le droit d'auteur sur les jeux Nintendo et sous licence Nintendo*⁴³².

428. - CJUE, 23 janvier 2014, *Nintendo Co. Ltd c./ PC Box Srl*, C-355/12.

429. - §15 de la décision.

430. - §26 de la décision, interprétant l'article 6 §3 de la directive 2001/29 précitée.

431. - Considérant 48 de la directive 2001/29 précitée.

432. - §36.

La Cour se contente donc de mettre en avant les critères qui devront être appliqués par les juridictions nationales. La question de savoir si une MTP est disproportionnée par rapport à l'objectif poursuivi est une question de fait, à laquelle une juridiction comme la CJUE n'a pas la possibilité de répondre de manière satisfaisante. C'est toute la différence avec le mécanisme américain, qui faisait appel à des acteurs aptes à se prononcer eux-mêmes, au niveau fédéral, sur la réalité du terrain et sur les équilibres de chaque secteur concerné – ce qui les avait conduit, rappelons-le, à admettre le *jailbreak* des téléphones, mais à refuser celui des consoles.

Par conséquent, la question du « droit au *jailbreak* » risque de recevoir des réponses divergentes dans les différents États de l'Union, ce qui n'est certainement pas une bonne solution au regard de la conception uniforme, au niveau mondial, des terminaux en cause. Il semble nécessaire que la Commission européenne prenne des initiatives sur ce terrain.

260. L'omniprésence à venir des terminaux - L'EFF formule un avertissement qui ne peut laisser indifférent :

(...) copyright is chipping away at your right to own devices you've bought and paid for —from e-books to toasters and even your car. Time and again, people who want to modify their own property or sell it to others are told that they can't, because their property comes saddled with copyrighted code they're not allowed to modify or give away when they are done with the device⁴³³.

Demain, tout sera « terminal ». Au fur et à mesure que « l'intelligence » attendue des objets s'accroîtra, ils seront dotés de couches logicielles de plus en plus perfectionnées, et éventuellement d'une connexion au réseau – c'est le fameux « Internet des objets ». Sous prétexte de protéger le capital intellectuel ainsi investi, on les criblera de mesures techniques de protection qui seront autant de restrictions au pouvoir du propriétaire d'en jouir et d'en disposer. Objets inanimés, vous avez bien une âme, le logiciel, un cheval de Troie qui fait entrer dans le monde tangible les problèmes jusqu'ici réservés aux biens culturels immatériels.

LA PROPRIÉTÉ : CONCLUSION

Le numérique a confirmé sa capacité à constituer un laboratoire des tensions et mutations qui affectent actuellement le droit de propriété.

Les infrastructures de télécommunication sont le théâtre d'un affrontement somme toute classique entre le propriétaire du matériel, qui prétend disposer de sa chose en toute liberté et véhiculer comme il l'entend les informations qui transitent par ses câbles, et l'intérêt général, qui

433. - K. Sheehan, « YODA, the Bill... », art. préc.

visait une « neutralité du réseau » propre à maximiser l'innovation, la concurrence et la liberté des utilisateurs. Les États-Unis d'Amérique sont en train d'arbitrer en faveur du premier, tandis que l'Europe s'oriente vers une défense plus affirmée du second.

Les infrastructures de coordination, comme le *Domain Name System*, ont constitué une illustration, hors de la sphère du droit de l'environnement, de l'intérêt que peut présenter la notion de biens communs, située aux antipodes d'une propriété individualiste et exclusive. Lorsque le contrôle de ces ressources a été relâché par l'administration américaine, une solution aurait consisté à en assurer une gouvernance publique mondiale, mais c'est une solution de droit privé qui a été retenue. L'ICANN, simple association sans but lucratif de droit californien, jusqu'alors sous tutelle, s'est retrouvée officiellement libre de sa gestion. Elle prétend œuvrer pour le bien commun en représentant de manière suffisamment diverse, au sein de ses organes dirigeants, les intérêts multiples et divergents mobilisés par Internet – c'est la *multistakeholder policy*. En pratique, il apparaît que cette représentation n'est ni exhaustive ni égalitaire, et qu'elle fait la part la plus belle à des intérêts académiques et commerciaux américains. Cela n'exclut pas nécessairement que les décisions prises soient les bonnes, car cette minorité a tout intérêt à préserver la ressource mondiale que constitue un Internet efficace et fonctionnel. Mais la question de la viabilité de long terme de ce modèle est posée.

Lorsqu'il s'est agi d'étudier la couche des contenus circulant sur les réseaux, c'est évidemment de propriété intellectuelle qu'il a été principalement question. Chacun sait qu'il existe un conflit entre la vocation même du réseau, qui est de permettre la reproduction et la circulation la plus facile des informations, et l'intérêt des titulaires de droits, qui est d'opérer une réservation efficace des utilités de leur création, de manière à en contrôler la distribution contre rémunération. Cette contradiction ne se résume pas au cliché du téléchargement massivement contrefaisant sur des réseaux de pair-à-pair. La logique propriétaire, dans une vision maximaliste, pourrait s'opposer à la simple mise en place non autorisée d'un lien vers page Web contenant une œuvre protégée par le droit d'auteur. Les règles de droit doivent alors être interprétées avec pragmatisme et souplesse. La propriété intellectuelle s'oppose également aux pratiques transformatives, courantes sur le réseau, qui usent d'une œuvre protégée comme d'un matériau pour réaliser un nouvel acte créatif. Là encore, des arbitrages délicats doivent être rendus entre protection des intérêts économiques des créateurs primaires, et intérêt général au foisonnement créatif dérivé. Le problème est cependant évité lorsque les titulaires de droits placent volontairement leur œuvre dans un fonds commun à disposition de tous. L'idéal des biens communs culturels est ainsi poursuivi non pas par un bannissement de la propriété, mais par son usage. Il est loisible au titulaire de ce droit de réaliser un

acte de disposition, pour relâcher volontairement son emprise sur sa chose et en ouvrir les utilités aux quatre vents. Cela revient à lui rendre en partie son statut initial de chose non rivale.

S'il constitue parfois une force contraire aux intérêts des titulaires de droits de propriété intellectuelle, le numérique constitue en d'autres occasions leur meilleur allié. La puissance des « mesures techniques de protection » est aujourd'hui considérable. Les droits des acheteurs de contenus culturels s'en trouvent diminués d'autant. Ils pouvaient auparavant revendre, prêter ou détruire leur exemplaire de l'œuvre, et tout simplement s'en servir sans demander périodiquement une autorisation à un serveur distant. Leurs droits étaient en réalité accrochés à un support physique qui tend à disparaître. Ils n'ont aujourd'hui accès aux utilités du bien immatériel que dans la stricte mesure d'autorisations précaires, et leur position ressemble davantage à celle d'un simple créancier dans le cadre d'un contrat de prestation de service qu'à celle d'un titulaire de droit réel. Pour inverser cette tendance, certains ont imaginé invoquer une propriété contre une autre : celle de l'exemplaire contre celle de l'œuvre. L'idée est prometteuse, mais elle a échoué jusqu'ici à s'imposer. Il faudra à l'avenir soit restaurer la puissance de cette propriété seconde pour tempérer celle des titulaires de droits d'auteur, soit basculer dans une logique de droit des contrats – ce qui impliquera de revoir certains concepts, comme celui de prohibition des engagements perpétuels.

Cet effritement du droit réel en matière de contenus culturels donne au premier abord raison à ceux qui estimaient que la propriété des choses tangibles diffère substantiellement de celle des choses immatérielles. Cette idée ne résiste toutefois pas à l'analyse du droit applicable aux terminaux. Ce terme désigne les appareils utilisés pour se connecter à Internet. La catégorie était autrefois restreinte aux ordinateurs, à certaines consoles et aux téléphones intelligents, mais elle s'ouvre au fur et à mesure du développement de « l'Internet des objets ». Réfrigérateurs, télévisions ou automobiles sont en train de basculer dans le monde des terminaux. Sous prétexte de protéger la propriété intellectuelle qu'ils renferment, ces biens tangibles sont eux aussi truffés de mesures techniques de protection matérielles et logicielles, susceptibles d'enfermer le bien dans un écosystème fermé de consommables et d'applications, de limiter ses fonctionnalités à celles autorisées par le fabricant et de requérir des autorisations périodiques de fonctionnement. Toute la construction de la propriété comme un droit immédiat, emprise directe sur la matière pouvant s'exercer sans le concours d'un tiers, est ainsi remise en cause. Un crépuscule des droits réels menace dans certains domaines. Quelles réponses faut-il apporter ? Le combat américain pour le « droit au jailbreak », dont le fondement ultime est la propriété du consommateur, pourrait nourrir la réflexion.

Troisième notion – Le contrat

261. **Le numérique : un monde contractuel meilleur ?** - Toutes les sociétés, si éloignées qu'elles fussent de la nôtre dans le temps et dans l'espace, ont pratiqué des échanges économiques. Il leur a donc fallu passer des contrats. Le contrat se retrouve partout, mais il n'est jamais vraiment le même : il est en effet « (...) trop profondément ancré dans la pratique, et son droit trop tributaire du contexte philosophique, politique, économique et juridique dans lequel il se développe, pour qu'on puisse raisonnablement identifier une notion de contrat intemporelle »¹.

L'étoile de la propriété est en train de pâlir, ainsi qu'il a été démontré précédemment. Celle du contrat brille d'autant plus vivement. La société numérique utilise sans posséder, loue plutôt qu'elle n'achète, se complaît dans « l'âge de l'accès ». Quand bien même sa soif de droits réels se ranimerait, les biens immatériels et les terminaux sont rétifs à l'exercice d'une emprise immédiate ; en fait de propriétés, ce sont des créances de long terme qui s'accumulent dans les patrimoines. Tout n'est qu'obligations. Au centre du droit civil numérique, le contrat trône en majesté. Il n'en est que plus important de déterminer quelles valeurs il véhicule aujourd'hui.

Le XIXe siècle affichait sa foi dans un contrat juste et émancipateur.

Les présupposés sous-tendant la conception dominante du contrat, au XIXe siècle et au début du XXe siècle, se conforment aux idées (...) de l'égalité des citoyens, de la rationalité des individus et de la poursuite par chacun de son intérêt. En premier lieu, en effet, les contractants seront considérés comme des personnes égales, au moins abstraitement (...). En deuxième lieu, les contractants seront considérés comme libres et, partant, comme capables de s'engager rationnellement, ou au moins raisonnablement. Ils seront censés s'imposer une obligation et entrer dans un contrat à l'issue d'une pesée des intérêts et d'un choix délibéré [...] »².

Le XXe siècle s'émancipe progressivement de cette vision enchantée et prend conscience de l'existence de contrats déséquilibrés, dans lesquelles une partie faible — le travailleur, puis le consommateur — doit être protégée contre une partie plus forte — l'employeur, le banquier, l'assureur, le « professionnel ». Sur le fondement du devoir de bonne foi, les obligations d'information et devoirs de conseil viennent peu à peu au secours d'individus prêts à succomber à tous les pièges, par ignorance et incompetence³.

1. - M. Latina, « Contrat : généralités » in *Répertoire civil Dalloz*, mai 2017, n° 1.

2. - J. Rochfeld, *Les grandes notions...*, op. cit., n° 7.2. Dans le même sens, V. par ex. P. Malaurie, L. Aynès et P. Stoffel-Munck, *Droit des obligations*, LGDJ, 8e éd., 2016, n° 392.

3. - J. Rochfeld, op. cit., n° 7.8.

Mais le numérique n'est-il pas en train de réaliser les visions des théoriciens libéraux du contrat ? L'individu, sincèrement désireux de se comporter en agent rationnel, ne manquait-il pas tout simplement de moyens à la hauteur de ses ambitions ? Si son regard est obscurci par de graves asymétries d'information, et qu'il ne trouve face à lui qu'un nombre limité de contreparties, il ne faut pas s'étonner qu'il prenne sur les marchés contractuels des positions peu efficaces⁴. En se connectant sur Internet, le candidat au contrat peut, en quelques instants et pour un coût négligeable, accéder à des dizaines d'offres pour le produit ou le service de son choix, assorties d'un descriptif précis et classées en fonction du prix demandé⁵. S'y ajoutent des dizaines d'avis de précédents clients, portant aussi bien sur l'objet même de la convention que sur le sérieux du futur partenaire contractuel. Par ailleurs, les échappatoires aux contrats déséquilibrés se multiplient : dans un vaste mouvement parfois appelé « économie collaborative », les particuliers s'achètent entre eux les repas, les transports ou les heures de bricolage qu'ils recherchaient auparavant auprès de professionnels. C'est le retour de la convention entre égaux.

Ces premières impressions favorables doivent être largement nuancées. Les changements entraînés par le numérique sont à la fois plus complexes et plus équivoques.

262. De la dématérialisation des transactions au triomphe des plateformes - Le changement le plus simple et le plus apparent dans la manière de contracter à l'ère numérique consiste en la dématérialisation des transactions. Théoriquement, un client pourrait conserver le même réseau de partenaires qu'il s'était constitué avant Internet, en interagissant simplement avec eux selon des modalités matérielles différentes. Il pourrait réserver un restaurant, une chambre d'hôtel et même acheter un livre à des prestataires locaux, qu'il connaissait déjà, en passant simplement par le réseau. À ce stade, les adaptations juridiques rendues nécessaires sont déjà complexes : comment s'assurer de l'identité des contractants à distance, comment conserver la preuve de leur convention, comment faire évoluer les moyens de paiement ? Ces problèmes pourraient sembler de pure intendance. Après tout, des difficultés similaires se posaient déjà lorsque la vente par correspondance était pratiquée par téléphone ou par fax. Mais l'évolution n'est peut-être pas uniquement formelle : consentir à un contrat, depuis son canapé, d'un double tapotement du pouce sur un téléphone, est-ce la même chose que de sortir de chez soi, se déplacer, pénétrer à l'intérieur d'un point de vente, insérer sa carte bancaire et taper son code – ou remplir un chèque ?

4. - Sur le rôle des asymétries d'information sur les marchés, V. par ex. l'un des plus célèbres articles par George A. Akerlof, « The Market for "Lemons": Quality Uncertainty and the Market Mechanism », *The Quarterly Journal of Economics*, Vol. 84, No. 3. (Aug., 1970), p. 488.

5. - En ce sens : A. Tabarrok et T. Cowen, « The end of asymmetric information ? », article cato-unbound.org du 6 avril 2015 ; G. Nasri, « Solving information asymmetry: how today's companies are empowering consumers and creating more efficient markets », article huffingtonpost.com du 9 septembre 2013.

Les nouveautés, bien évidemment, ne se cantonnent pas à cela. L'internaute est en mesure de comparer en ligne un grand nombre de propositions contractuelles – encore faut-il qu'elles soient présentées de manière honnête par le moteur de recherche, le comparateur ou l'offrant lui-même. Surtout, le champ de cette comparaison peut facilement s'élargir, lorsque le bien ou le service n'est pas attaché à un territoire précis : à un marché local — des libraires, par exemple — se substitue un marché national, voire international. En parallèle, la puissance des intermédiaires numériques est telle qu'ils peuvent inclure dans leurs résultats les propositions de très petits acteurs, y compris non professionnels, dont la visibilité aurait sans cela été insuffisante, et dont l'offre de contrat se serait perdue dans les limbes. Ainsi, le numérique ne se contente pas d'influer sur les formes concrètes que revêt l'acte de contracter : il exerce des pressions très fortes sur la structure de l'offre de biens et de services, qu'il fait évoluer en profondeur.

Plus important encore, il attribue un rôle d'une importance inédite aux intermédiaires. Des millions d'internautes sillonnent en permanence la toile à la recherche de contrats alléchants. Mais il ne suffit pas de combiner une myriade de sites d'entrepreneurs isolés ou de PME avec des moteurs de recherche généralistes pour parvenir à des processus efficaces. De là vient le rôle des plateformes, qui organisent la rencontre d'une offre et d'une demande plus ou moins spécialisées : ventes immobilières, transport automobile en covoiturage ou par un professionnel, logement de vacances, œuvres d'art... Le pouvoir de donner ou de retirer un référencement aux candidats au contrat, de mettre en valeur ou de marginaliser une proposition donne aux intermédiaires un poids totalement inédit. Le métier de l'entremise existe depuis longtemps, mais c'est un phénomène récent et découlant directement du numérique que celui qui leur donne le poids économique le plus important au sein de la relation tripartite qui s'instaure. La distribution de l'information est consacrée comme le métier le plus important dans la chaîne de valeur. On assiste à un renouvellement d'anciennes figures contractuelles, comme le courtage, qui leur confère un rayonnement sans précédent.

Pour étudier l'ensemble de ces évolutions de fond et de forme du droit des contrats, il est expédient de recourir à une classification bien connue, qui oppose les règles communes à toutes les conventions (section 1) et celles qui sont spéciales à certains contrats (section 2).

Section 1 – Droit commun des contrats

Le contrat sera regardé ici en sa qualité d'outil universel, apte aux échanges économiques de toutes natures. L'impact du numérique apparaîtra par conséquent à son plus haut niveau de généralité.

Il n'a jamais été aussi facile ni aussi rapide de conclure un contrat, à n'importe quelle heure du jour où de la nuit, sans avoir à se déplacer ni à se confronter à aucun interlocuteur humain. Cette simplicité constitue sans nul doute un progrès, mais elle n'est pas sans présenter quelques dangers. Dans de telles conditions, les lourds enjeux dont le pacte peut être porteur se laissent volontiers oublier, et la parole peut être donnée avec une légèreté excessive (I). Le contraste est alors frappant avec la rigueur implacable dont le contrat numérique pourrait faire l'objet au stade de son exécution, si certaines innovations récentes devaient se développer (II).

I – L'idéal de fluidité dans la conclusion des contrats

263. **Faire vite, faire simple** - La priorité avouée des professionnels du commerce électronique consiste à maximiser leur « taux de conversion ». Il s'agit de transformer un maximum de visiteurs de leur site — souvent attirés par une publicité ciblée, qui représente un coût par clic — en clients payants. Tous les choix techniques et juridiques opérés visent à faciliter au maximum ce passage à l'acte. Il en résulte une certaine fragilité du consentement au contrat (A) aussi bien que des preuves du contrat (B).

A – La fragilité du consentement au contrat

264. **Le mirage du consentement plus éclairé** – Le numérique étant synonyme d'information abondante et peu coûteuse, nous avons vu qu'il pourrait être perçu comme un instrument susceptible d'améliorer significativement l'efficacité des marchés. Par le passé, le futur client devait se contenter d'offres contractuelles locales, peu nombreuses, dont la seule collecte coûtait temps et énergie. À présent, dit-on, une simple requête lancée sur les réseaux le rendrait omniscient. Hélas, ce tableau idyllique ne correspond pas la réalité⁶.

Tout d'abord, rien ne sert d'embrasser le monde des biens et services tout entier d'un regard, s'il est contemplé à travers des verres déformants. Or, l'internaute n'a pas accès à une connaissance

6. - D. Aurebach, « Internet n'a pas résolu par magie les imperfections des marchés », article *slate.fr* du 15 juin 2015.

neutre et directe des offres contractuelles : il s'en remet à un moteur de recherche ou à une plateforme, qui pourrait facilement tirer profit de sa position pour biaiser l'information au profit de partenaires ou au détriment d'adversaires. Cette question sera abordée plus loin⁷.

Ensuite, même à supposer que les intermédiaires se soient montrés parfaitement loyaux, la facilité de comparaison montre rapidement ses limites. Savoir que tel appareil photo est vendu par six marchands et pouvoir classer les propositions par ordre croissant de prix, livraison incluse, est certes utile. Mais encore faudrait-il comparer les conditions générales de vente de ces différents sites pour s'assurer que les détails plus fins de la transaction sont eux aussi satisfaisants. La complexité augmente encore si l'on bascule dans le monde des contrats s'étalant dans la durée, principalement constitué de prestations de services. Leurs caractéristiques ne se comparent pas toujours aisément – quiconque a déjà choisi une mutuelle de santé sur la base d'informations récoltées en ligne en a conscience. Enfin, il faut souligner que beaucoup de grands services du monde numérique ont peu ou pas de concurrents, en raison des effets de réseau déjà évoqués et de l'effet « *winner takes all* » : il n'y a dans ce cas ni comparaison ni alternative. Ces prestataires sont d'autant plus libres de rédiger des contrats d'adhésion particulièrement rigoureux.

Internet n'est peut-être pas la matrice d'un monde contractuel plus juste. Faut-il aller jusqu'à affirmer l'inverse ? Les dangers que présente la conclusion inconsidérée d'un contrat ne sont évidemment pas propres au monde numérique. On trouve hors-ligne des conventions aux stipulations byzantines et des paroles trop vite prononcées. Comme souvent, le numérique ne fait qu'exacerber, condenser, amplifier des phénomènes qui l'ont précédé. Mais cela suffit néanmoins à faire grandir les périls. Alors même que les offres de contrat y sont souvent complexes (1), elles font l'objet d'un processus d'acceptation d'une grande simplicité (2).

1. - La complexité des offres

265. **Plan** - Si les internautes acceptent sans difficulté de payer pour des biens, ils ont été accoutumés à profiter de services sophistiqués sans bourse délier. Il n'y a pas là l'expression d'une philanthropie propre à la Silicon Valley, mais bien plutôt le triomphe de *business models* typiques du réseau⁸. Les utilisateurs le comprennent-ils toujours ? Le risque d'un malentendu sur ce qui constitue l'économie même du contrat est réel (a). Par ailleurs, quand bien même l'architecture

7. - V.infra, n°318.

8. - Sur cette spécificité : G. DangNguyen, S. Dejean et T. Pénard, « Gratuité sur internet : entre logiques individuelles et logiques communautaires », in *La gratuité. Un concept aux frontières de l'économie et du droit*, LGDJ, 2013, p. 91

globale de la convention aurait été bien comprise, c'est dans le détail des stipulations que le danger se tapit parfois (b).

a – L'économie générale du contrat : des gratuités factices

266. **Les « gratuités intéressées »** - Sur la page d'accueil de Facebook, l'une des plus visitées au monde, un formulaire invite les inquiétants marginaux qui ne seraient pas encore membres du réseau social à s'inscrire sans tarder. Une mention rassurante s'étale en caractères apparents : « C'est gratuit (et ça le restera toujours) ».

« Gratuit » : le mot interpelle. Madame Zolynski rappelle cependant qu'il importe de distinguer la gratuité « pure - proche du sens religieux : l'oubli de soi, le don divin » de la gratuité « intéressée », qui n'est qu'une stratégie au service d'un fin égoïste⁹.

L'article 1107 du Code civil n'entretient aucune illusion sur ces gratuités de façade, qui dispose : « Le contrat est à titre onéreux lorsque chacune des parties reçoit de l'autre un avantage en contrepartie de celui qu'elle procure. Il est à titre gratuit lorsque l'une des parties procure à l'autre un avantage sans attendre ni recevoir de contrepartie ». Ainsi, il ne suffit pas de constater une absence de facturation du service pour que le contrat soit considéré comme « à titre gratuit ». Il faut s'attacher à la notion de « contrepartie », qui ne se réduit pas aux prestations en argent. Mieux : le texte disqualifie la gratuité lorsqu'une contrepartie est simplement « attendue », alors même qu'elle ne serait pas (encore ?) reçue. Ainsi le Code sépare-t-il nettement le monde des libéralités de celui des échanges économiques. Les modèles que l'on s'apprête à décrire relèvent assurément de la seconde catégorie. Simplement, dans certains cas, la contrepartie est discrète ; dans d'autres, elle est différée.

267. **Les contreparties discrètes : la monétisation de soi** - La gratuité dont elle prétend relever, la société Facebook ne s'est pas contentée d'en faire un slogan : elle l'a transformée en argument juridique, dans une affaire soumise à la Cour d'appel de Paris. Dans un litige qui l'opposait à l'un de ses utilisateurs, elle avait invoqué une clause attributive de juridiction au profit d'une juridiction de Santa Clara, en Californie. La stipulation étant menacée par des dispositions impératives du Code de la consommation, le réseau social ne craint pas d'affirmer « (...) que le contrat n'est pas un contrat de consommation en raison de la gratuité de son service ». La Cour ne fut pas convaincue,

9. - C. Zolynski, « La gratuité en questions », in *La gratuité. Un concept aux frontières de l'économie et du droit*, LGDJ, 2013, p.XI, V. P. XIII.

qui releva que « (...) la société Facebook Inc retire des bénéfices importants de l'exploitation de son activité »¹⁰.

Alors que le modèle d'affaires d'une société comme Apple repose plus classiquement sur le paiement, par sa clientèle, de ses biens et services, ses concurrents Google ou Facebook constituent les exemples plus connus d'un système de financement des prestations offertes aux utilisateurs par les tiers. Des données à caractère personnel sont recueillies en grand nombre, qui seront soit cédées aux tiers, qui les exploiteront par eux-mêmes, soit utilisées par la société à l'origine de la collecte pour constituer un « profil » précis. Celui-ci constituera le support d'annonces publicitaires personnalisées, les emplacements étant alors attribués aux annonceurs par des systèmes d'enchères.

L'importance pratique prise par ces contrats a été relevée par une proposition de directive européenne « concernant certains aspects des contrats de fourniture de contenu numérique »¹¹. Le champ d'application du futur texte est ainsi défini :

« La présente directive s'applique à tout contrat par lequel un fournisseur fournit un contenu numérique au consommateur ou s'engage à le faire, en échange duquel un prix doit être acquitté ou une contrepartie non pécuniaire, sous la forme de données personnelles ou de toutes autres données, doit être apportée de façon active par le consommateur »¹².

Le texte est intéressant, en ce qu'il reconnaît que céder à une société commerciale des fragments de son intimité revient à payer, à défaut d'un prix — terme technique renvoyant au paiement d'une somme d'argent, notamment dans le cadre d'un contrat de vente — une contrepartie ayant elle aussi sa valeur¹³. On remarquera toutefois que ce sont toutes les « données » qui sont visées, au-delà de celles présentant un caractère personnel¹⁴.

Puisque la proposition de directive vise à consacrer de nouvelles protections au profit des consommateurs, il est important d'en faire profiter les clients qui « paient en données » : sans cela,

10. - CA Paris, 12 février 2016, pôle 02 ch. 02, arrêt n° 201658.

11. - (La notion de « contenu numérique » est d'invention récente et ne se laisse pas facilement saisir. V. Notamment V.-L. Bénabou, « Entrée par effraction d'une notion juridique nouvelle et polymorphe : le contenu numérique », *Dalloz IP/IT*, 2017 p. 7.

12. - Proposition de la Commission européenne en date du 9 décembre 2015, 2015/0287 (COD), art. 3 al. 1. Nous soulignons. Sur cet article de la proposition, V. J. Rochfeld, « Le “contrat de fourniture de contenus numériques” : la reconnaissance de l'économie spécifique “contenus contre données” », *Dalloz IP/IT*, 2017, p. 15

13. - Considérant 13 de la directive précitée : « Dans l'économie numérique, les acteurs du marché ont souvent et de plus en plus tendance à considérer les informations concernant les particuliers comme ayant une valeur comparable à celle de l'argent. Il est fréquent que du contenu numérique soit fourni, non pas en échange d'un paiement, mais moyennant une contrepartie non pécuniaire, c'est-à-dire en accordant l'accès à des données à caractère personnel ou autres. »

ces contrats profiteraient d'un avantage concurrentiel par rapport à ceux dans lesquels on paie en argent¹⁵.

Le projet semble jusqu'ici à l'abri des critiques. Mais l'inquiétude naît à la lecture d'un considérant, qui précise : « [...] la présente directive devrait exclusivement s'appliquer aux contrats en vertu desquels le fournisseur demande des données, comme un nom et une adresse électronique ou des photos, et le consommateur les lui communique **de façon active**, directement ou indirectement [...] »¹⁶. Dès lors ne seraient concernées ni « [...] la localisation si elle est nécessaire au bon fonctionnement d'une application mobile [...] », ni « [...] les informations recueillies et transmises par un cookie, sans que le consommateur ne les ait fournies activement, même si le consommateur accepte le cookie ». Un auteur estime à juste titre que cela vide le texte de sa substance, les données personnelles recueillies passivement étant couramment les plus importantes, d'un point de vue tant qualitatif que quantitatif¹⁷.

Ainsi, le législateur européen lui-même commence tout juste à prendre conscience de la spécificité de ces contrats « service contre données », et peine à en contenir les dérives potentielles. Il est alors à craindre qu'à plus forte raison, les simples utilisateurs n'aient pas conscience des termes véritables de l'échange auquel ils se soumettent. L'apparence de gratuité que certains opérateurs laissent prospérer suffit probablement à endormir les méfiances les moins aiguës.

Un autre modèle d'affaires présente une physionomie propre à entretenir une certaine confusion dans l'esprit du public : celui du *freemium*.

268. Les contreparties différées : les modèles freemium - Le concept du *freemium* est très habile. Il peut être expliqué ainsi : « Un produit ou un service gratuit est fourni au consommateur dans l'objectif de renforcer son intérêt pour un produit ou un service payant : le consommateur doit payer s'il entend accéder au produit ou service soit de meilleure qualité soit dans son intégralité »¹⁸. Depuis quelques années, il s'impose comme le modèle d'affaires dominant dans les services Internet et applications mobiles ; son importance au sein des start-up aurait même dépassé le modèle précédemment décrit, reposant sur la publicité ciblée et les données personnelles, inventé

14. - J. Rochfeld, « Le “contrat de fourniture de contenus numériques”... », art. préc.

15. - Considérant 13 de la proposition de directive précitée : « Établir une distinction en fonction de la nature de la contrepartie serait discriminatoire pour certains modèles commerciaux. Cela inciterait inutilement les entreprises à s'orienter vers une offre de contenu numérique en contrepartie de données ».

16. - Considérant 14 de la directive précitée. Souligné par nous.

17. - J. Rochfeld, « Le “contrat de fourniture de contenus numériques”... », art. préc.

18. - C. Zolynski, « La gratuité en questions... », art. préc., p. XIV.

dans les années 2000¹⁹. Le système ne mérite pas d'être fustigé dans son principe. Lorsqu'une société comme Dropbox offre des comptes utilisateurs gratuits de stockage de données de type *cloud computing*, elle affiche sans ambiguïté qu'un espace limité sera disponible. Le client séduit par le service, mais dont les besoins en ressources seront plus importants, décidera ensuite de sortir son portefeuille ; de même que celui qui aura découvert la prestation pour son usage personnel, mais qui voudra ensuite y recourir dans un cadre professionnel. Bien d'autres usagers s'en tiendront pour toujours à la version gratuite, sans en éprouver de frustration particulière.

D'autres *freemium* adoptent un fonctionnement plus complexe. Beaucoup de jeux vidéo dits « *free-to-play* » relèvent de cette catégorie. Candy Crush Saga en constitue un exemple bien connu du grand public : il met en place des mécanismes de récompense du joueur qui produisent des effets proches de l'addiction, puis oblige régulièrement celui qui ne souhaite pas payer à une longue interruption avant de poursuivre sa partie. La frustration suscitée est si puissante qu'elle convainc une partie des utilisateurs de payer pour la faire cesser. D'autres jeux, qui organisent des affrontements directs entre participants, octroient un avantage décisif à ceux qui ont accepté de sortir leur carte bleue. Ainsi, c'est au cours de l'expérience de jeu que l'utilisateur découvre l'existence et la puissance des facteurs qui vont l'amener à rémunérer une expérience initialement présentée comme gratuite. La méthode est d'autant plus inquiétante qu'elle vise souvent de jeunes adolescents, voire des enfants, qui sont probablement moins à même de percevoir les manipulations dont ils font l'objet et d'y résister efficacement²⁰. Ici encore, il est à craindre que l'offre contractuelle ne soit pas totalement comprise avant d'être acceptée.

Dans les situations qui viennent d'être décrites, c'est le fonctionnement global du contrat, son économie générale, qui risque de faire l'objet d'un malentendu. Mais il arrive couramment, par ailleurs, que les dangers se tapissent dans les détails de la convention.

b – Les stipulations détaillées : l'omniprésence de clauses trompeuses

269. Des contrats sous influence américaine – Il n'est évidemment pas nécessaire de se rendre en ligne pour rencontrer des contrats d'adhésion — rédigés unilatéralement par une partie et non négociables — contenant des clauses particulièrement déséquilibrées²¹. La spécificité de l'univers

19. - V. Kumar, « Make freemium work », *Harvard Business Review*, mai 2014.

20. - Sur le *free-to-play* dans son ensemble : M. Rose, « Chasing the Whale: Examining the ethics of free-to-play games », article *gamasutra.com* du 9 juillet 2013 ; J. Hameau et al., « Why do players buy in-game content? An empirical study on concrete purchase motivations », *Computers in Human Behavior*, vol. 68, mars 2017, p. 538.

21. - L'article 1110 al. 2 du Code civil, dans sa rédaction issue de l'ordonnance 2016-131 du 10 février 2016, définit le contrat d'adhésion comme « (...) celui dont les conditions générales, soustraites à la négociation, sont

en ligne vient peut-être de ce que les géants du secteur sont pour la plupart implantés aux États-Unis d'Amérique : les conditions générales d'utilisation de leurs services en portent la marque, au point de constituer parfois de simples traductions en langue française des *terms of service* en vigueur outre-Atlantique.

Certaines clauses attributives de juridiction en constituent une première marque. Nous avons dit que Facebook avait exigé d'un utilisateur français, simple particulier, qu'il aille plaider devant un tribunal californien²². À présent, la société prend des précautions et précise : « si vous résidez dans un pays où la loi prévoit la compétence des tribunaux de votre pays de résidence, les litiges relatifs à la présente Déclaration ou à Facebook pourront être portés devant les tribunaux compétents de votre pays de résidence. Dans le cas contraire, vous porterez toute plainte, action en justice ou contestation [...] afférente à cette Déclaration ou à Facebook exclusivement devant un tribunal américain du Northern District de Californie ou devant un tribunal d'État du comté de San Mateo [...] »²³. Ainsi, c'est à l'internaute profane de procéder aux recherches nécessaires pour déterminer si une loi impérative de son pays le protège. C'est donc qu'un contrat standard a été rédigé pour être simplement traduit en différentes langues, et que le service juridique pour la France n'a pas cru nécessaire de l'adapter au droit européen, qui proscrit une telle stipulation dans les relations de consommation²⁴. Il est évident que de telles recherches ne peuvent être attendues du grand public, et que le seul fait d'entretenir une telle confusion constitue un problème en soi. D'autres plateformes se dispensent de toute réserve sur l'illégalité éventuelle de leur clause attributive de juridiction, comme Pinterest, qui renvoie elle aussi à une juridiction californienne et ne craint pas d'ajouter cet incroyable commentaire : « La Baie de San Francisco est magnifique à cette époque de l'année. Peu importe la saison d'ailleurs, c'est ce qui en fait un si bel endroit ! Et si vous voulez nous poursuivre en justice, c'est ici que cela se fera »²⁵.

Le traitement réservé aux données personnelles est une autre manifestation de l'origine américaine de nombreuses conditions générales. Ignorant purement et simplement les exigences européennes en la matière, la même société Facebook — qui n'est pas la seule à agir ainsi, mais qui mérite d'être citée en tant qu'acteur de tout premier plan — écrit, dans ses conditions générales : déterminées à l'avance par l'une des parties ».

22. - CA Paris, 12 février 2016, pôle 02 ch. 02, arrêt n° 201658, précité.

23. - Article 15 des conditions générales datées du 9 décembre 2016, toujours en vigueur en août 2017

24. - Règlement (CE) n° 44/2001 du Conseil du 22 décembre 2000 concernant la compétence judiciaire, la reconnaissance et l'exécution des décisions en matière civile et commerciale, article 16.1 : « 1. L'action intentée par un consommateur contre l'autre partie au contrat peut être portée soit devant les tribunaux de l'État membre sur le territoire duquel est domiciliée cette partie, soit devant le tribunal du lieu où le consommateur est domicilié ».

25. - Article 11 des conditions générales du 1^{er} novembre 2016, en vigueur en août 2017.

« Vous acceptez que vos données personnelles soient transférées et traitées aux États-Unis »²⁶. Cette fois-ci, la précaution n'est pas même prise de formuler une réserve quant au fait qu'une telle exigence pourrait contrevenir à la réglementation locale : le contrat donne une représentation trompeuse du droit applicable²⁷.

C'est encore le droit européen en matière de responsabilité des intermédiaires techniques, longuement évoqué au cours de l'étude, qui est ignoré dans les conditions générales de certaines grandes plateformes²⁸. Le contrat proposé par Twitter porte actuellement la clause suivante : « les entités twitter ne sauraient être tenues responsables d'aucun dommage indirect, accessoire, spécial, consécutif ou punitif, d'aucune perte de bénéfices ou de revenus, directe ou indirecte, d'aucune perte de données, privation de jouissance ou dépréciation du fonds de commerce, ni d'aucune autre perte intangible, qui résulteraient [...] (ii) du comportement ou du contenu d'une tierce partie dans les services, y compris, sans s'y limiter, d'un comportement diffamatoire, offensant ou illicite de la part d'autres utilisateurs ou tierces parties [...] »²⁹. Un peu plus loin, on peut certes lire que « Certaines juridictions n'autorisent pas l'exclusion des garanties implicites ou les limitations de durée des garanties implicites ; dans l'éventualité où, de ce fait, les clauses de limitation de responsabilité ci-dessus ne s'appliqueraient pas à vous dans leur intégralité, elles s'appliqueront dans la mesure maximale permise par la loi applicable ». Les termes mêmes qui sont employés trahissent le fait que le texte n'a pas été écrit pour notre droit, par exemple le mot « juridiction », maladroitement traduit de l'anglais *jurisdiction* et qui ne s'emploie guère ainsi dans la langue française³⁰. Par ailleurs, il s'agit d'une nouvelle manifestation de la méthode consistant à laisser planer le doute sur la légalité de clause, en laissant à l'utilisateur le soin de procéder aux recherches nécessaires. On trouve cependant pire : la société Instagram, par exemple, affirme sereinement : « Vous acceptez le fait qu'Instagram n'est pas responsable du Contenu publié sur le Service et qu'il

26. - Article 16 des mêmes conditions générales. Le droit de l'Union pose pourtant des conditions drastiques à de tels transferts, qui appelaient à l'évidence une certaine prudence dans la formulation : V.supra, n° 75

27. - Certes, les dispositions relatives aux données personnelles sont précédées d'une vague pétition de principe : « Nous nous efforçons de créer une communauté sans frontières avec des standards cohérents pour tous, tout en respectant les lois locales ». Mais la phrase précitée sur le transfert aux USA est immédiatement précédée de celle-ci : « Les clauses ci-après s'appliquent aux internautes qui interagissent avec Facebook en dehors des États-Unis ». Cela ne ressemble nullement à une réserve.

28. - V.supra, n°155.

29. - Article 5 des conditions générales dans leur révision du 30 septembre 2016.

30. - L'intuition se vérifie par la consultation des *terms of service* applicables aux États-Unis : « *some jurisdictions do not allow exclusion of implied warranties or limitations on the duration of implied warranties, so the above disclaimers may not apply to you in their entirety, but will apply to the maximum extent permitted by applicable law* ». Il s'agit bien d'une traduction mot-à-mot.

ne le cautionne pas. Instagram n'est aucunement obligé de présélectionner, de contrôler, de modifier ou de supprimer le Contenu »³¹. L'illégalité est manifeste.

Enfin, la difficulté d'acclimater ces contrats de culture américaine sous nos latitudes se révèle par la manière dont sont traitées les questions de propriété intellectuelle. Les droits concédés par l'utilisateur du service sur les contenus qu'il y publie sont souvent extrêmement larges. Le réseau social Delicious, qui ne dispose pas pour l'heure d'une version de ses conditions d'utilisation en langue française, prévoit ainsi : « *When you put User Content on the Service, you do give us (and our service providers, partners and other users) free and unlimited rights to use your User Content as part of the Service including as the Service may evolve in the future. This means we can use, including copying, modifying etc. what you put on the Service [...]* »³². Si elle est peut-être valable sous le régime du copyright, une licence aussi large est incompatible avec le principe de spécialité des cessions et, surtout, avec le droit moral de l'auteur tels qu'on les connaît en droit français de la propriété intellectuelle³³. Des plateformes disposant de conditions générales en langue française affichent des stipulations du même ordre³⁴.

270. Les réactions des pouvoirs publics – Au sein des services proposés sur Internet, la Commission des clauses abusives a choisi de passer au crible les conditions générales des réseaux sociaux. Elle a considéré que l'ensemble des stipulations qui viennent d'être présentées, et bien d'autres encore, créent un déséquilibre significatif entre les droits et obligations des parties³⁵. De telles clauses, lorsque la recommandation a été publiée, étaient abusives entre professionnels et consommateurs³⁶. Mais depuis, la réforme du droit des contrats est allée plus loin et répute non écrite toute clause qui crée un tel déséquilibre « dans un contrat d'adhésion », ce qui ne fait que renforcer encore l'intérêt des analyses menées par la Commission³⁷.

31. - Article 8, section « droits » des conditions d'utilisation en date du 19 janvier 2013, en vigueur en août 2017.

32. - *Delicious Terms of Service*, non datés, en vigueur en août 2017.

33. - V.supra, n°226.

34. - Ainsi Pinterest prévoit-il, au 2.b de ses conditions générales datées du 1^{er} novembre 2016 (en vigueur en août 2017) : « Vous accordez à Pinterest et à ses utilisateurs une licence mondiale non exclusive, libre de droits, transférable, avec possibilité de sous-licence, pour utiliser, stocker, afficher, reproduire, enregistrer, modifier, exécuter et distribuer votre contenu utilisateur, et créer des œuvres dérivées à partir de ce dernier sur Pinterest, uniquement dans le but de gérer, de développer, de fournir et d'utiliser les produits Pinterest ».

35. - Recommandation n° 14-02 : contrats de fourniture de services de réseaux sociaux.

36. - Ancien art. L. 132-1 C. conso., devenu art. L. 212-1, qui dispose en son premier alinéa : « Dans les contrats conclus entre professionnels et consommateurs, sont abusives les clauses qui ont pour objet ou pour effet de créer, au détriment du consommateur, un déséquilibre significatif entre les droits et obligations des parties au contrat ».

37. - Art. 1171 al. 1 C. civ.

Toutefois, les exemples cités plus haut sont tous tirés de conditions générales actuellement en vigueur : les stipulations litigieuses n'ont visiblement pas toutes été retirées des modèles de contrats, tant s'en faut. En juin 2017, La Commission européenne s'est agacée des résistances durables des grandes sociétés du numérique s'agissant de la conformité de leurs conditions générales au droit de l'Union, et a adressé à certaines d'entre elles des courriers lourds de menaces, dont nous verrons s'ils sont suivis d'effets³⁸.

En attendant, les utilisateurs de ces services qui liraient les offres contractuelles avant de les accepter seraient trompés sur la réalité du droit applicable. Mais ces utilisateurs n'existent pas : personne ne lit véritablement les conditions générales. Cela n'est pas nécessaire à l'acceptation du contrat.

2 – La simplicité de l'acceptation

271. Les formes adoptées par la rencontre des volontés en ligne – Une sous-section spécifique du Code civil est consacrée à la conclusion du contrat lorsqu'elle a lieu par voie électronique. Ses exigences sont peu nombreuses, et d'une parfaite banalité.

Le professionnel proposant la conclusion de biens ou de services en ligne doit rendre ses stipulations accessibles d'une façon qui permette de les conserver ou de les reproduire. Aussi longtemps qu'elles sont accessibles par voie électronique « de son fait », il reste engagé³⁹. Certaines mentions obligatoires sont attendues⁴⁰. Leur nombre augmente singulièrement dans le cas d'un contrat de consommation⁴¹.

Le législateur utilise le mot « offre » pour désigner cette proposition de contracter, mais la doctrine souligne à juste titre que si le professionnel se réserve la possibilité de valider ou non une commande après étude, c'est le client qui se trouvera véritablement en position d'offrant, tandis que le commerçant en ligne sera exceptionnellement l'acceptant⁴².

38. - J. Fioretti, « EU increases pressure on Facebook, Google and Twitter over user terms », article *reuters.com* du 24 juillet 2017.

39. - Article 1127-1 du Code civil.

40. - Même texte : « 1° Les différentes étapes à suivre pour conclure le contrat par voie électronique ; 2° Les moyens techniques permettant au destinataire de l'offre, avant la conclusion du contrat, d'identifier d'éventuelles erreurs commises dans la saisie des données et de les corriger ; 3° Les langues proposées pour la conclusion du contrat au nombre desquelles doit figurer la langue française ; 4° Le cas échéant, les modalités d'archivage du contrat par l'auteur de l'offre et les conditions d'accès au contrat archivé ; 5° Les moyens de consulter par voie électronique les règles professionnelles et commerciales auxquelles l'auteur de l'offre entend, le cas échéant, se soumettre ». L'article 1127-3 précise qu'il est fait exception à ces exigences s'agissant des contrats conclus exclusivement par échange de courriers électroniques (al. 1) ou conclus entre professionnels (al. 2).

41. - Art. L. 224-27 et s. C. conso., qui procèdent à de multiples renvois.

42. - P. Stoffel-Munck, « LCEN. La réforme des contrats du commerce électronique », *CCE*, sept. 2004, étude

Que doit faire le client quant à lui pour accepter – ou, exceptionnellement, formuler l’offre ? Le Code civil prévoit que « Le contrat n’est valablement conclu que si le destinataire de l’offre a eu la possibilité de vérifier le détail de sa commande et son prix total et de corriger d’éventuelles erreurs avant de confirmer celle-ci pour exprimer son acceptation définitive » : c’est la formalité connue sous le nom de « double clic »⁴³. Le nom n’est pas très heureux, puisqu’il renvoie en informatique à l’ordre donné par deux clics de souris réalisés en un court instant, alors qu’il s’agit bien, ici, de presser un premier bouton, d’accéder à un nouvel écran récapitulatif qu’il faut lire afin de vérifier que tout est conforme, avant de cliquer sur un second bouton⁴⁴. La référence opérée par le texte au « prix total » laisse entendre que la formalité a été conçue en contemplation des contrats payés en argent, sans égard pour ceux dans lesquels la contrepartie est différente, notamment lorsqu’elle consiste en un accès à des données personnelles. Cela n’est pas très grave, car ce que vérifie le client qui achète un livre ou un abonnement à un magazine, c’est la quantité d’articles placés dans son panier, et la somme d’argent réclamée en contrepartie. Dans le cas des contreparties en données, et en l’état du système, la seule relecture pertinente devrait porter sur les conditions générales ou la politique de confidentialité. Or, quel que soit le contrat considéré, ces documents ne font l’objet que d’une attention au mieux faible, et souvent nulle.

272. Le désintérêt pour le contenu précis du contrat – La proposition contractuelle devrait ensuite entrer contact avec l’intellect du client, et faire l’objet d’un examen suffisant. C’est très rarement le cas : une décision de la CJUE en constitue une intéressante illustration.

Un concessionnaire automobile allemand avait acheté un véhicule sur Internet. Il assigna son cocontractant devant une juridiction de son pays, mais on lui opposa une convention attributive de juridiction en faveur d’un tribunal belge. L’allemand estimait que la clause ne revêtait pas une forme écrite, contrairement aux exigences du règlement Bruxelles I. En effet, il soutenait que « (...) que la page Internet de la défenderesse au principal contenant les conditions générales de vente de celle-ci ne s’ouvre pas automatiquement lors de l’enregistrement ni lors de chaque opération

30. Dans le cas d’un contrat passé entre un professionnel et un non-professionnel ou consommateur, cet examen tendant à valider la commande ne saurait être discrétionnaire. La Commission des clauses abusives rappelle « qu’un certain nombre de conditions générales de vente prévoient la possibilité pour le vendeur de refuser au consommateur, pour quelque raison que ce soit, la possibilité de confirmer l’acceptation de l’offre ; que ces clauses qui contreviennent à l’article L 122-1 du code de la consommation, sont illicites » (Recommandation n°07-02 relative aux contrats de vente mobilière conclus par Internet, 4°. Recommandation consultable sur www.clauses-abusives.fr).

43. - Article 1127-2 du Code civil. Sur cette acceptation : H. Causse, « Le contrat électronique, technique du commerce électronique », in *Le contrat électronique. Au cœur du commerce électronique, journées d’études organisées par le DJCE de Poitiers*, LGDJ, 2005, p. 11 ; D. Noguero, « L’acceptation dans le contrat électronique », même ouvrage, p. 49.

44. - La manœuvre supposant deux clics dans un court intervalle s’écrit certes double-clic, avec un tiret, mais cette nuance ne peut être saisie à l’oral.

d'achat. Au contraire, il faudrait sélectionner un champ contenant l'indication «cliquer ici pour ouvrir les conditions générales de livraison et de paiement dans une nouvelle fenêtre» (technique d'acceptation par «clic» dite «du click-wrapping») »⁴⁵. La CJUE décide que :

Dans l'affaire au principal, il n'est pas contesté que la technique d'acceptation par « clic » rend possibles l'impression et la sauvegarde du texte des conditions générales en question avant la conclusion du contrat. Dès lors, la circonstance que la page Internet contenant ces conditions ne s'ouvre pas automatiquement lors de l'enregistrement sur le site Internet et lors de chaque opération d'achat ne saurait remettre en cause la validité de la convention attributive de juridiction⁴⁶.

Quoique professionnel, cet internaute s'était donc contenté de cocher une case prétendant qu'il avait lu les conditions générales, alors qu'il ne l'avait pas fait. Les stipulations ne lui en étaient pas moins opposables. Chacun d'entre nous a déjà procédé de même, et recommencera⁴⁷.

D'ailleurs, afficher systématiquement le contrat et obliger l'internaute à le dérouler jusqu'au bout, comme c'est parfois le cas, constituerait-il une quelconque amélioration ? La longueur et l'austérité de certains textes auraient raison des juristes professionnels les plus endurants – sans même parler du grand public. Les conditions générales iTunes furent longtemps célèbres pour leur volume approchant les soixante pages⁴⁸.

Dans ce contexte, faire défiler un ascenseur, cliquer sur une case à cocher ou sur un bouton constituent des gestes dénués de toute signification intellectuelle véritable, des rituels accomplis par pur automatisme. Les expériences visant à le démontrer, avec plus ou moins d'humour, ne manquent pas. Une étude empirique a démontré que 98 % des 500 internautes croyant s'inscrire à un réseau social avaient ignoré une clause des conditions générales par laquelle ils acceptaient de partager leurs données avec la NSA et leurs employeurs, et promettaient d'offrir leur enfant

45. - CJUE, 21 mai 2015, C-322/24, *Jaouad El Madjoub c./ CarsOnTheWeb. Deutschland GmbH* : D., 2015, 2031, obs. L. d'Avout et S. Bollée ; *ibid.*, 2016, 1045, obs. H. Gaudemet-Tallon et F. Jault-Seseke ; *AJCA*, 2015, 370, obs. L. Constantin ; *RTD com.*, 2015, 777, obs. A. Marmisse-d'Abbadie d'Arrast. Cet argument de l'acheteur est présenté au §14 de la décision.

46. - §39 de la décision précitée.

47. - Certes, un arrêt antérieur nuance cette conclusion s'agissant des mentions relatives au droit de la consommation, qui ressortissent de la directive n° 1997/7/CE du 20 mai 1997 relative à la protection des consommateurs en matière de contrats à distance, bien distincte du règlement Bruxelles I. Certaines mentions ne peuvent faire l'objet d'un simple renvoi par lien hypertexte et doivent être présentées au client sans qu'il ait à accomplir de démarche active, fût-elle un simple clic : CJUE, 5 juillet 2012, C-49/11, *Content Services Ltd c./ Bundesarbeitskammer* : *AJ contrats d'affaires*, 2015, p. 370, obs. L. Constantin. Il s'agissait en l'espèce des informations relatives au droit de rétractation. On les fera alors apparaître quelque part sur un écran de confirmation, ou dans un mail.

48. - V. par ex. U. Pidaparthi, « What you should know about iTunes' 56-page legal terms » article *cnn.com* du 6 mai 2011. Ces conditions générales ont été un objet de railleries récurrents, jusqu'à être adoptées sous forme de longs comics : R. Sikoryak, *Terms and conditions*, Drawn and Quarterly, 2017.

premier-né à titre de paiement⁴⁹. Autre expérience : une entreprise avait inclus dans son contrat une clause promettant une récompense de 1000 dollars au premier utilisateur qui la réclamerait. Cela a pris quatre mois⁵⁰. Plus inattendu : les conditions générales Amazon Web Services contiennent aujourd'hui encore une clause qui, après avoir posé une restriction d'utilisation à un produit, précise :

« (...) cette restriction ne s'appliquera pas dans le cas (certifié par les Centres compétents des États-Unis pour le contrôle des maladies) d'une infection virale étendue transmise par des morsures ou par le contact avec des fluides corporels impliquant que des cadavres humains reviennent à la vie et cherchent à consommer de la chair humaine vivante, du sang, des tissus cérébraux ou nerveux et pourrait aboutir à la chute d'une civilisation organisée »⁵¹.

Bien sûr, le phénomène consistant à ne pas lire ses contrats est ancien et connu⁵². Mais la conclusion d'une convention hors-ligne introduit une certaine pesanteur, bienvenue. Le contrat fait sentir, physiquement, son poids et son volume. Et puis, si l'on excepte les petits contrats de la vie courante, un interlocuteur humain est présent, apte à répondre à des questions, exécutant son éventuel devoir de conseil en partie par la parole, et non uniquement par l'insertion d'une soixante-et-unième page, qui ne sera pas lue, à un document déjà obèse.

Alors sur Internet, comment peut-on faire mieux ? Deux pistes peuvent être explorées : densifier le consentement ou le dépasser.

273. Densifier le consentement – Qui reste attaché à une rencontre effective des volontés comme fondement du contrat souhaitera redonner de l'épaisseur à l'acceptation. Elle devrait être précédée d'une prise de connaissance des conditions générales qui soit d'une durée raisonnable, et cependant véritablement éclairante.

Une première piste est explorée par les professionnels des biens et services en ligne eux-mêmes. Certains d'entre eux ont entrepris d'assortir le texte complet de leur contrat d'une version abrégée et simplifiée, plus accessible au profane. La démarche paraît louable dans son principe, mais se révèle très vite problématique dans ses modalités d'application. Les conditions générales de Pinterest peuvent à nouveau servir d'exemple. Sous une clause limitative de responsabilité particulièrement complexe, le résumé suivant est proposé :

49. - J. A. Obar et A. Oeldorf-Hirsch, « The biggest lie on the internet: ignoring the privacy policies and terms of service policies of social networking services », article du 25 août 2016 disponible sur *papers.ssrn.com*.

50. - L. Magid, « It pays to read license agreements », article *pcpitstop.com*, date non précisée.

51. - Conditions *Amazon Web Services* en date du 19 avril 2017, article 57.10.

52. - V. déjàsupra, n°64.

« Nous élaborons le meilleur service possible pour vous, mais nous ne pouvons pas promettre qu'il sera parfait. Nous ne sommes pas responsables de certaines choses. Si vous pensez que nous le sommes, nous tenterons de gérer les choses de la façon la plus sensée possible »⁵³.

Les pertes de sens par rapport au texte d'origine sont à l'évidence beaucoup trop importantes pour qu'une telle version simplifiée soit utile. Le fait que les deux textes émanent du même rédacteur pose par ailleurs la question de savoir s'ils ne sont pas tous les deux opposables au professionnel. Enfin, dans la mesure où il ne s'agit pas d'un commentaire indépendant, on ne peut évidemment attendre de la version allégée qu'elle dénonce les stipulations illégales du texte initial. On se souvient que sous une clause attributive de juridiction vraisemblablement illicite face à un consommateur, Pinterest proposait une « version simplifiée » ironisant sur le charme qu'il y avait à partir plaider dans la baie de San Francisco⁵⁴.

Aussi une autre piste, sans doute plus intéressante, consiste à confier à un tiers indépendant le soin de rédiger un résumé des conditions générales. Il peut s'agir d'une association à but non lucratif : c'est le cas dans le projet anglophone « *Terms of Service ; Didn't Read* »⁵⁵. Les conditions générales des principaux services sur Internet y sont en cours d'analyse. Une note générale leur est attribuée, de « *class A* » pour les plus vertueuses à « *class E* » pour les plus dangereuses. Aussi et surtout, cette note fait l'objet d'une motivation synthétique, qui prend la forme d'un résumé des droits attribués ou dénués aux utilisateurs, assorti de pictogrammes⁵⁶. Les concepteurs proposent aux internautes d'installer un module additionnel pour leur navigateur, qui leur permettra, le moment venu, d'accéder facilement à cette couche d'information en surimpression des conditions générales classiques. Il est clair, ici, que le résumé n'engage en rien le professionnel, dans la mesure où il est rédigé par un tiers. Mais si le travail est sérieusement mené, par suffisamment d'individus compétents et motivés, le résultat peut être d'une grande qualité : c'est un exemple de *crowdsourcing*.

Mais tant qu'à accepter le principe d'une expertise des conditions générales menée par un tiers, et dont les résultats synthétiques seront accessibles au public, ne faudrait-il pas tout simplement les demander à un service de l'État, comme la Commission des clauses abusives ou la CNIL ? Cela

53. - Conditions générales Pinterest, en date du 1^{er} novembre 2016, encore en vigueur en août 2017, commentaire sous l'article 9.

54. - V.supra, n°269.

55. - Le projet et l'équipe sont présentés à la page <http://tosdr.org/about.html>.

56. - De la même façon, la fondation Mozilla proposait de résumer les politiques de confidentialité en matière de données personnelles à l'aide de pictogrammes : V.supra, n°64.

semblera à certains trop interventionniste. Et pourtant, la seule alternative au renouveau du consentement se situe alors dans le dépassement du consentement.

274. Dépasser le consentement – Si les internautes ne s'inquiètent pas de ce qu'une clause de condition générale puisse leur réclamer leur enfant premier-né à titre de paiement d'un service, c'est sans doute parce qu'ils font confiance à leur système juridique pour priver une telle clause de tout effet. Les consommateurs, tout du moins, s'offrent probablement le luxe d'un désintérêt pour le contrat à l'abri de ce qu'ils pensent être, à tort ou à raison, une solide législation d'ordre public. Ainsi considéré, le processus contractuel s'éloigne d'une rencontre des volontés privées pour se transformer en une interaction entre un pouvoir privé et un encadrement public. Ce phénomène est tout simplement celui du contrat d'adhésion, que le numérique n'inaugure pas, mais qu'il amplifie, en donnant à des contrats de moins en moins lus un rayonnement de plus en plus large. La doctrine contractualiste a déjà mis en garde contre ses dangers à de nombreuses reprises⁵⁷. Pourquoi, dans ces conditions, une recommandation de la Commission des clauses abusives comme celle relative aux réseaux sociaux reste-t-elle plusieurs années sans effet concret ? La puissance publique semble encore rechigner à se mêler du contrat privé, peut-être à tort.

La rapidité et la facilité avec lesquelles les contrats dématérialisés sont conclus ont sans aucun doute des vertus, mais nous avons vu qu'elles entraînaient une certaine faiblesse du consentement. Constatons à présent qu'elles ont aussi des effets en matière de preuve du contrat.

B – La fragilité des preuves du contrat

275. Le poids du commerce électronique – Le chiffre d'affaires du commerce électronique pour l'année 2016 s'établit à 72 milliards d'euros : le double de ce qu'il représentait à peine cinq ans plus tôt⁵⁸. Cette impressionnante statistique laisse pourtant de côté les contrats de prestation de service conclus en contemplation d'une contrepartie non monétaire, comme l'accès à des données personnelles. On imagine que des échanges économiques d'une telle ampleur ne pourraient avoir lieu sans le soutien d'un droit de la preuve parfaitement adapté, manié par les professionnels avec la plus grande rigueur, de sorte qu'il soit toujours possible de démontrer en justice que telle convention affichant tel contenu a été conclue entre telles parties⁵⁹. Est-ce bien le cas ?

57. - Par ex. J. Calais-Auloy, « L'influence du droit de la consommation sur le droit civil des contrats », *RTD. civ.*, 1994, p. 239.

58. - Fédération e-commerce et vente à distance (FEDAV), *Les chiffres clés 2016/2017*.

59. - Les développements qui vont suivre sont largement nourris de notre étude « Réflexions sur la preuve et l'imputabilité des contrats électroniques », *RLDI*, janvier 2013, n° 89, p. 78.

Le droit français s'est attaché à fournir les textes nécessaires. Le droit de la preuve littérale fut d'abord refondu par une loi du 13 mars 2000 portant adaptation du droit de la preuve aux technologies de l'information et relative à la signature électronique⁶⁰, loi complétée par un décret d'application relatif à la signature électronique⁶¹. Dès lors, il devenait possible d'utiliser un écrit numérique aussi bien qu'un écrit papier... du moins lorsqu'un écrit était exigé à titre de preuve, et non érigé en condition de validité. Cette ultime infériorité de l'écrit électronique fut rapidement gommée : une loi du 21 juin 2004 pour la confiance dans l'économie numérique permit qu'on l'utilisât y compris lorsqu'il était requis *ad validitatem*⁶². Le même texte donna naissance à un chapitre du Code civil consacré aux contrats électroniques. Ledit chapitre fut remanié et complété par une ordonnance du 16 juin 2005 relative à l'accomplissement de certaines formalités contractuelles par voie électronique⁶³. Enfin, la récente réforme du droit des contrats déplaça les textes dans le plan du Code, sans en altérer la substance⁶⁴.

Ce vaste arsenal législatif et réglementaire est-il propre à procurer une parfaite sécurité juridique aux professionnels et consommateurs désireux de conclure des transactions par voie électronique ?

276. Preuve par le client - Nous avons déjà vu selon quelles modalités les volontés de l'offrant et de l'acceptant sont supposées se rencontrer sur le terrain électronique⁶⁵. Après cela, « L'auteur de l'offre doit accuser réception sans délai injustifié et par voie électronique de la commande qui lui a été ainsi adressée »⁶⁶. Chacun se souvient avoir reçu un tel message électronique, après une commande, dans un délai qui ne dépasse généralement pas quelques secondes : cette brièveté manifeste l'automatisation totale du procédé dans les grandes enseignes du commerce en ligne. La doctrine souligne que cet accusé de réception pourra servir de preuve au client, au cas où son

60. - Loi n° 2000-230, sur laquelle V. not. : F. Schwerer, « Réflexions sur la preuve et la signature dans le commerce électronique », *CCE*, déc. 2000, chron. 16.

61. - Décret n° 2001-272.

62. - Loi n° 2004-575. Cette loi transposait elle-même une directive du 8 juin 2000, n° 2000/31/ce, du parlement européen et du conseil, *relative à certains aspects juridiques des services de la société de l'information, et notamment du commerce électronique, dans le marché intérieur*. Sur cette loi, V. not. P. Stoffel-Munck, « LCEN. La réforme des contrats du commerce électronique », art. préc. ; J. Rochfeld, « La loi n° 2004-575 du 21 juin 2004 pour la confiance en l'économie numérique », *RTD. civ.*, 2004, p. 574.

63. - Ordonnance n° 2005-674.

64. - Ordonnance n° 2016-131 du 10 février 2016 portant réforme du droit des contrats, du régime général et de la preuve des obligations. Aujourd'hui, le chapitre consacré à la « formation du contrat » (chapitre II, sous-titre 1^{er}, titre III du Code civil) consacre des « dispositions propres au contrat conclu par voie électronique » dans sa section 3 « la forme du contrat », aux articles 1174 et s.

65. - V. *supra*, n°271.

66. - Art. 1127-2 du Code civil.

partenaire refuserait de s'exécuter, en niant l'existence du contrat⁶⁷. Est-ce aussi simple ? Tout d'abord, le législateur n'a pas indiqué quelle sanction il entendait voir appliquer au cybermarchand qui négligerait d'envoyer de tels accusés de réception. Si un client suit toutes les étapes du processus de commande, mais ne reçoit ensuite aucun accusé, que pourra-t-il faire ? Pour démontrer que son partenaire contractuel est fautif de ne lui avoir rien envoyé, il faudra qu'il prouve qu'il y avait contrat... ce qui était précisément l'objet du document non reçu⁶⁸ ! Le recours à des captures d'écran, parfois suggéré, pose de multiples problèmes : l'écran qui récapitule le contenu du panier et précède le second et dernier clic ne démontre rien ; l'écran suivant se contente souvent de féliciter l'acheteur pour le succès de « la commande », sans détailler son contenu. Surtout, ces captures d'écran sont très aisément falsifiables⁶⁹. C'est pourquoi il a été proposé, à juste titre, de rendre obligatoire le caractère entièrement automatisé et quasi instantané des envois d'accusés de réception. Si telle est la pratique des plus grandes enseignes, on peut craindre qu'elle n'ait pas été adoptée par l'intégralité des 204 000 sites marchands français⁷⁰. Les services de la répression des fraudes devraient pouvoir procéder à des tests de commande. Si ce problème des accusés de réception était résolu, les clients disposeraient contre les vendeurs ou prestataires indéclicats d'un document écrit, émanant de l'autre partie, ce qui écarterait toute difficulté probatoire les concernant⁷¹.

277. Preuve par le marchand ou la plateforme - Mais qu'en est-il du problème inverse : celui de la preuve que devrait rapporter un commerçant en ligne ou une plateforme ? La question n'est pas sans intérêt. Que l'on songe au client qui nie avoir passé le contrat dont le cybermarchand se prévaut. Plusieurs explications sont possibles. Premièrement : il est de mauvaise foi, et cherche seulement à ne pas exécuter son engagement. Deuxièmement : le contrat n'existe effectivement pas, par exemple faute de deuxième clic, mais le commerçant en ligne prétend le contraire. Troisièmement : une personne a usurpé l'identité du client apparent pour passer la commande : le marchand va alors alléguer l'existence d'un contrat contre ledit client apparent, qui va devoir se défendre. Dans cette dernière hypothèse, le problème de preuve rejoint la question de l'imputabilité du contrat électronique, particulièrement épineuse : comment savoir qui tient la souris⁷² ?

67. - P. Stoffel-Munck, « LCEN. La réforme... », art. préc. ; D. Noguero, « L'acceptation... », art. préc.

68. - *Ibid.*

69. - C'est le problème, de manière générale, des procédés des preuves que l'on se constitue à soi-même, dont il sera question infra, n°286.

70. - Fédération e-commerce et vente à distance (FEDAV), *Les chiffres clés 2016/2017*, précités.

71. - Ajoutons qu'au-delà d'un certain montant, le droit de la consommation fait peser sur le marchand une obligation d'archiver une trace de la transaction et de la tenir à disposition du consommateur. V. sur ce point C. Feral-Schuhl, *Cyberdroit*, op. cit., n° 51.25.

72. - En ce sens, l'aphorisme : « Sur Internet, personne ne sait que vous êtes un chien ! », cité par T. Piette-

Il est assez naturel d’imaginer que les règles gouvernant les questions de preuve des contrats électroniques sont à puiser dans les réformes récentes, précédemment décrites, et dont l’objectif affiché était de faire basculer le droit des obligations français dans l’ère du numérique. La réalité est tout autre : la preuve littérale électronique est largement délaissée (1). Ce sont des modes de preuve anciens, dits « imparfaits », qui occupent la plus grande place en pratique (2).

1. – La place marginale de la preuve littérale électronique

278. **Preuve littérale** - L’idéal, pour un commerçant en ligne, serait d’être en mesure de se prévaloir d’une preuve littérale. Une telle preuve est en effet requise lorsque la transaction porte sur une valeur supérieure ou égale à 1500 euros ; de plus, quelle que soit la valeur en litige, il ne peut être prouvé contre ou outre un écrit que par écrit⁷³. Ce dernier «[...] consiste en une suite de lettres, de caractères, de chiffres ou de tous autres signes ou symboles dotés d’une signification intelligible, quel que soit leur support »⁷⁴. À une conception matérielle, physique, de l’écrit et du support papier, qui fut la nôtre des millénaires durant, on a en effet récemment substitué une acception bien plus large, basée sur le sens, l’intelligibilité. Peu importe que l’information soit fixée sur un support à l’aide d’encre, ou qu’elle circule par voie hertzienne, par satellite ou le long de fils de cuivre.

Cette belle pétition de principe, selon laquelle tous les supports se valent, ne peut cependant occulter plusieurs difficultés majeures⁷⁵. D’abord, l’information sous forme électronique est souvent stockée sur des supports qui en permettent la modification instantanée, illimitée et discrète⁷⁶. Ensuite, nous avons déjà souligné les redoutables difficultés qui tiennent à l’identification en ligne des individus.

279. **Écrit électronique et signature électronique** - L’article 1366 du Code civil tente de répondre à ces préoccupations : « L’écrit électronique a la même force probante que l’écrit sur support papier, sous réserve que puisse être dûment identifiée la personne dont il émane et qu’il soit établi et conservé dans des conditions de nature à en garantir l’intégrité ».

Coudol, « L’identité des personnes, les certificats et la signature électronique », *CCE*, janv. 2005, étude 2.

73. - Art. 1359 C. civ. La somme de 1500 euros a été fixée par le décret n° 2004-836 du 20 août 2004, art. 56.

74. - Comp., avant l’ordonnance de 2016, l’art. 1316 du Code civil : « La preuve littérale, ou preuve par écrit, résulte d’une suite de lettres, de caractères, de chiffres ou de tous autres signes ou symboles dotés d’une signification intelligible, quels que soient leur support et leurs modalités de transmission ».

75. - C. Castets-Renard, « Le formalisme du contrat électronique ou la confiance décrétée », *Defrénois*, 2006, n° 20, p. 1529 ; M. Mekki, « Le formalisme électronique : la “neutralité technique” n’emporte pas “neutralité axiologique” », *RDC*, 2007, n° 3, p. 681 ; A. Hollande, *Pratique du droit de l’informatique*, op. cit., n° 1719.

76. - C’est notamment le cas lorsqu’elle est stockée sous forme magnétique, par exemple sur un disque dur. Même certains CD ou DVD gravés sont « réinscriptibles ».

Dire cela change tout, tant il est difficile en pratique de réunir de telles conditions. Il existe bien un moyen : la signature électronique. Après avoir tenté de fusionner, en une définition unique, toutes les formes d'écrit, le Code civil essaie d'envelopper de même, en un seul mouvement, le concept de signature. L'art. 1367 1 pose sobrement : « La signature nécessaire à la perfection d'un acte juridique identifie son auteur. Elle manifeste son consentement aux obligations qui découlent de cet acte [...]. ». L'alinéa 2 entreprend ensuite d'adapter la notion au monde numérique : « Lorsqu'elle est électronique, elle consiste en l'usage d'un procédé fiable d'identification garantissant son lien avec l'acte auquel elle s'attache. La fiabilité de ce procédé est présumée, jusqu'à preuve contraire, lorsque la signature électronique est créée, l'identité du signataire assurée et l'intégrité de l'acte garantie, dans des conditions fixées par décret en Conseil d'État. ».

280. Désaffection pratique pour la signature électronique « présumée fiable » - Le décret a été pris et renvoie largement à un règlement européen⁷⁷. Concrètement, le système rend nécessaire le recours à un tiers certificateur, et à un chiffrement asymétrique avec utilisation d'une paire de clés publiques et privées⁷⁸. Nous avons déjà présenté ces techniques, qui sont au fondement des procédés d'identification les plus fiables sur Internet. Elles sont employées dans le *Transport Layer Security* (TLS) pour s'assurer que la connexion est établie avec un site authentique et non avec un usurpateur⁷⁹. À l'heure actuelle, deux raisons s'opposent à leur utilisation quotidienne dans le commerce électronique.

La première est d'ordre technique. Rappelons-nous comment une banque, une administration ou un webmarchand obtient un certificat TLS : son identité est vérifiée hors-ligne par un tiers de confiance, qui se fait présenter les documents nécessaires. La confiance ainsi obtenue est propagée

77. - Un premier décret n° 2001-272 avait été pris le 30 mars 2001. Il a été remplacé par un décret n° 2017-1416 du 28 septembre 2017 relatif à la signature électronique. Celui-ci renvoie pour l'essentiel au règlement (UE) n° 910/2014 du Parlement européen et du Conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur. Dans son annexe II, le règlement énumère des exigences techniques élevées, notamment : « a) la confidentialité des données de création de signature électronique utilisées pour créer la signature électronique est suffisamment assurée ; b) les données de création de signature électronique utilisées pour créer la signature électronique ne peuvent être pratiquement établies qu'une seule fois ; c) l'on peut avoir l'assurance suffisante que les données de création de signature électronique utilisées pour créer la signature électronique ne peuvent être trouvées par déduction et que la signature électronique est protégée de manière fiable contre toute falsification par les moyens techniques actuellement disponibles ; d) les données de création de signature électronique utilisées pour créer la signature électronique peuvent être protégées de manière fiable par le signataire légitime contre leur utilisation par d'autres ». Sur ce texte et la manière dont les exigences européennes pourraient évoluer à l'avenir, V. not. A. Penneau, « La preuve des actes électroniques en droit français. Conséquences du règlement européen e-IDAS », *JCP E*, n° 20, 18 mai 2017, 1264.

78. - V. not. M. Videau, « Aspect techniques de la preuve littérale reposant sur l'écrit électronique », *RLDI*, 2009, n° 52, supplément spécial, p. 15 ; L. Grynbaum, « La preuve littérale. Dispositions générales. Ecrit électronique », in *Juris-Classeur civil*, art. 1316 à 1316-4, fasc. 10, décembre 2016, n° 50.

79. - V. *supra*, n° 41.

en ligne dans un second temps. En France, du côté des utilisateurs des plateformes, ces procédures n'ont été appliquées qu'à des professionnels de certains secteurs, notamment celui des marchés publics⁸⁰. Les individus ordinaires ne disposent d'aucune clé de chiffrement issue d'une telle procédure d'identification, et ne peuvent donc pas s'en servir pour signer. En Belgique par exemple, nous avons expliqué que l'État avait joué le rôle du tiers de confiance, en fournissant à ses administrés une carte d'identité électronique contenant une clé de chiffrement personnelle précisément destinée à la signature de contrats⁸¹.

Mais même alors subsiste le second problème, qui relève des stratégies commerciales. Dès que le processus de conclusion de la transaction en ligne est un tant soit peu alourdi, le « taux de conversion » baisse, car des clients éventuels sont découragés. Par paresse ou incompétence, ils abandonnent le processus de commande. Les professionnels du commerce en ligne préfèrent se contenter de preuves bien plus frustes, et du risque contentieux qui les accompagne, s'il en résulte une hausse du chiffre d'affaires⁸². En faveur de cet arbitrage, il faut ajouter que la mise en place de signatures chiffrées représente un coût, qui serait parfois sans rapport avec le faible montant des transactions passées.

Ainsi, dans le domaine du commerce en ligne destiné au grand public, personne n'a recours à la signature électronique présumée fiable⁸³. Le « double clic » utilisé par le client des grandes enseignes de la vente sur Internet ne peut en aucun cas s'analyser comme une signature électronique présumée fiable au sens du Code civil. La Commission des clauses abusives a d'ailleurs relevé que : « diverses conditions générales confèrent à l'acceptation par “double clic” la même valeur qu'une signature électronique, sans autre précision, alors qu'un tel processus contractuel ne répond pas nécessairement aux exigences du décret du 30 mars 2001 relatif à la signature électronique, de telle sorte qu'en laissant croire au consommateur qu'il est présumé engagé par une signature ne répondant pas aux exigences légales, une telle stipulation est de nature à créer un déséquilibre significatif à son détriment »⁸⁴.

281. Des signatures électroniques à fiabilité démontrée ? - Afin de présenter les textes applicables, nous sommes partis de l'écrit électronique, avons relevé qu'il doit offrir certaines

80. - V. par ex. G. Clamour, « La signature électronique dans les marchés publics », *Contrats et marchés publics*, 2012, n° 8, p. 25.

81. - V. *supra*, n°44.

82. - Ce constat est dressé de la manière la plus nette par Christophe Davy, dirigeant du secteur du commerce en ligne : V. l'entretien en annexe de notre étude précitée « Réflexions sur la preuve... ».

83. - C. Castets-Renard, *Droit de l'Internet...*, *op. cit.*, n° 424.

84. - Recommandation n°07-02 relative aux contrats de vente mobilière conclus par Internet, précitée, 6°.

garanties de fiabilité, constaté que ces garanties de fiabilité peuvent résulter de l'apposition d'une signature électronique fiable, et exposé que cette fiabilité est présumée en cas de respect des prévisions d'un décret pris en Conseil d'État. Remontons à présent ces textes en sens inverse. Il est acquis que la conclusion d'un contrat électronique sur une plateforme de type Amazon, FNAC, ou Rue du commerce n'obéit pas aux exigences du décret. Il pourrait néanmoins s'agir d'une signature électronique, s'il est malgré tout démontré par la partie qui s'en prévaut que le procédé d'identification employé était fiable⁸⁵. La plupart des commandes passées à partir d'un ordinateur relié à Internet reposent sur la création d'un compte utilisateur, auquel est associé un mot de passe. Ce mot de passe pourrait-il être assimilé à une forme de signature électronique ? Cela semble exclu : il relie l'acte passé non pas à une personne identifiée, mais à un compte utilisateur, dont seule l'adresse email fait l'objet d'une vérification à la création⁸⁶. L'intitulé de cette adresse email peut ne contenir aucune référence au nom de l'utilisateur réel, voire afficher le nom d'une tierce personne physique. Il en va de même des champs « nom » et « prénom » du compte utilisateur, qui sont purement déclaratifs. Enfin, il est généralement possible de laisser indéfiniment active l'identification du compte sur un poste informatique donné, de sorte que le mot de passe n'aura plus à être fourni lors des prochaines commandes passées depuis ce poste. Décidément, un tel procédé n'évoque en rien la signature électronique voulue par le législateur.

Ne pourrait-on être en présence, malgré l'absence de signature à proprement parler, d'un écrit électronique au sens de l'article 1366 du Code civil ? Rappelons que ce texte exige notamment « que puisse être dûment identifiée la personne dont il émane ». Il faudrait donc que le cybermarchand puisse produire un document émanant de son client. Or, il n'en dispose pas⁸⁷. Le double clic va laisser une trace dans les serveurs informatiques de cette entreprise. Ce qu'il sera possible de produire, c'est un extrait du journal interne du serveur, un fichier que les informaticiens désignent habituellement par le terme anglais de *log*. Émanant de la personne même qui entend apporter une preuve, ce document ne peut être considéré comme un « écrit électronique ».

85. - A. Ayewouadan « La preuve des actes juridiques sous le prisme des contrats électroniques », *RLDI*, 2009, n° 45, p. 73, spéc. n° 31.

86. - Un lien est envoyé par email, sur lequel il faut cliquer pour démontrer qu'on est bien le titulaire de l'adresse électronique indiquée, ce qui sera crucial pour le commerçant au moment de satisfaire à son obligation d'accuser réception des commandes par voie électronique.

87. - Si le marchand prétendait disposer d'un écrit électronique, le client n'aurait qu'à opposer une dénégation. Dans ce cas, le juge est forcé de vérifier « si les conditions, mises par les articles 1366 et 1367 du code civil à la validité de l'écrit ou de la signature électroniques, sont satisfaites » (art. 287 du CPC, relatif à la vérification d'écriture, dont l'alinéa 2 ici cité a été adapté au problème de l'écrit électronique).

282. **La chaîne de blocs : une preuve d'avenir ?** - Il n'est pas possible d'aborder la question des preuves numériques sans évoquer la « chaîne de blocs » ou *blockchain*, une technologie qui provoque actuellement une intense curiosité doctrinale⁸⁸. Elle a pu être définie comme suit :

*La blockchain est une technologie de stockage et de transmission d'informations, fonctionnant grâce à un système distribué et des procédés cryptographiques. Ce grand journal public, contenant l'historique de tous les échanges effectués entre les utilisateurs depuis sa création, est partagé et constamment vérifié ; son mode de gouvernance, par consensus distribué, le rend en principe infalsifiable. Chaque utilisateur peut ainsi participer à son bon fonctionnement en vérifiant la validité de la chaîne de blocs de transactions et prendre connaissance des transactions effectuées, ce qui en garantit la publicité et la traçabilité*⁸⁹.

Le seul texte français qui y fait actuellement référence la dénomme « dispositif d'enregistrement électronique partagé »⁹⁰. L'origine de la *blockchain* est à rechercher dans la monnaie électronique Bitcoin. Savoir qui possède ces devises et pour quel montant revient à tenir un registre mondial, permanent, et exhaustif des transactions en bitcoins. Deux grandes méthodes sont alors envisageables. La première, classique, consiste à s'en remettre à un tiers de confiance déterminé. La seconde, innovante, dissémine dans les machines de milliers d'utilisateurs des automatismes associés à des techniques de chiffrement, capables de se coordonner sans la moindre intervention centralisée pour stocker des morceaux du journal et en vérifier l'intégrité à tout instant. La confiance n'est plus localisée ni personnifiée : vaporisée en gouttelettes microscopiques, elle se trouve partout à la fois. C'est la même approche générale qui avait entraîné le passage d'un réseau

88. - V. not. : C. Zolynski, « La *blockchain* : la fin de l'ubérisation ? », *Dalloz IP/IT*, 2017, p. 385 ; D. Legeais, « Blockchain », fasc. préc. ; D. Legeais, « La blockchain », *RTD. com.*, 2016, p. 830 ; S. Drillon, « La révolution Blockchain », *RTD. com.*, 2016, p. 893 ; X. Delpech, « La délicate appréhension de la Blockchain par le droit », *AJ contrat*, 2017, p. 244 ; O. Hielle, « La technologie Blockchain : une révolution aux nombreux problèmes juridiques », *Dalloz actu.*, 31 mai 2016 ; Y. Cohen-Adria, « Blockchain : révolution ou évolution ? », *Dalloz IP/IT*, 2016, p. 537 ; Y. Moreau et C. Dornbierer, « Enjeux de la technologie de blockchain », *D.*, 2016, p. 1856 ; G. Marraud des Grottes, « La blockchain : un secteur encore en phase d'exploration, mais très prometteur... », *RLDI*, 2017, n° 138 ; T. Verbiest, « Technologies de registre distribué (blockchain) : premières pistes de régulation », *RLDI*, 2016, n° 129 ; G. Canivet, « Blockchain et régulation », *JCP E*, 2017, n° 36, 1469 ; P.-J. Benghozi, « Blockchain : objet à réguler ou outil pour réguler ? », *JCP E*, 2017, n° 36, 1470 ; P. De Filippi, « What Blockchain means for the sharing economy », *Harvard Business Review*, 15 mars 2017. Les articles traitant principalement de la blockchain sous l'angle des *smart contracts* seront cités infra, n°302.

89. - C. Zolynski, « La *blockchain* : la fin de l'ubérisation ? », art. préc. L'auteur précise que cette définition correspond aux blockchains publiques. Il en existe aussi « (...) qui fonctionnent sur le modèle d'un réseau privé dont le gérant peut modifier le protocole quand il le juge utile, et dont l'accès et l'utilisation sont limités à un certain nombre d'acteurs ».

90. - Art. L. 223-12 du Code monétaire et financier : « Sans préjudice des dispositions de l'article L. 223-4, l'émission et la cession de minibons peuvent également être inscrites dans un **dispositif d'enregistrement électronique partagé permettant l'authentification de ces opérations**, dans des conditions, notamment de sécurité, définies par décret en Conseil d'État » (nous soulignons). La même terminologie est employée par un « projet d'ordonnance blockchain/titres financiers » de la Direction générale du Trésor (septembre 2017) : <https://www.tresor.economie.gouv.fr/Articles/2017/09/19/consultation-publique-projet-d-ordonnance-blockchain-titres-financiers>.

de communication téléphonique centralisé à l'architecture souple et distribuée d'Internet⁹¹. Chaque fois qu'un ensemble de transactions a été passé, il est relaté dans un bloc d'information qui sera relié à celui qui le précède et à celui qui le suivra par des techniques de chiffrement. Le journal, qui est accessible à tout intéressé, se construit à partir de la toute première transaction, par empilement de strates successives⁹². Le caractère totalement infalsifiable du registre devrait être considéré avec prudence : dans le domaine de la sécurité informatique, rien n'est invulnérable. Les auteurs prudents se contentent de qualifier la technologie « d'extrêmement robuste »⁹³.

Le fonctionnement qui vient d'être décrit permet de figer dans le marbre numérique une information quelconque. De multiples usages peuvent alors être imaginés, dont certains intéressent à l'évidence le droit des preuves. Ainsi, conserver une description horodatée d'une création de l'esprit, par le texte ou par l'image, permettrait à un auteur de démontrer aux tiers l'antériorité de son droit. Une chaîne de blocs pourrait servir de registre d'état civil, ou de livre foncier, ou de répertoire des testaments. On pourrait encore, et c'est le point qui nous intéresse ici, confier à sa mémoire supposée infaillible le souvenir de la conclusion d'un contrat et de son contenu. Il est parfois affirmé qu'une convention cristallisée dans une *blockchain* constitue nécessairement un écrit électronique au sens du Code civil, une preuve littérale parfaite⁹⁴. L'affirmation est inexacte. Rappelons que « L'écrit électronique a la même force probante que l'écrit sur support papier, sous réserve que puisse être dûment identifiée la personne dont il émane et qu'il soit établi et conservé dans des conditions de nature à en garantir l'intégrité »⁹⁵. Il est vrai qu'une chaîne de blocs conserve en principe les informations dans des conditions de nature à garantir l'intégrité. En revanche, rien dans son fonctionnement par défaut n'assure que l'identité des personnes à l'origine de la transaction a été sérieusement vérifiée. Le registre est totalement aveugle au monde qui l'entoure. S'il est capable de conserver une trace pérenne d'un contrat dont on lui dit qu'il a été passé entre Dupont et Durand, il n'a aucune capacité à déterminer par lui-même si ces noms correspondent à une identité réelle, s'ils sont usurpés ou s'ils constituent des pseudonymes. Une interface avec le monde social et juridique lui est nécessaire. À cette étape, le recours à un tiers de confiance ne peut

91. - V.supra, n° 8 s.

92. - Il s'agit du fonctionnement d'une *blockchain* « publique ». Des chaînes de bloc privées existent par ailleurs, qui ne seront pas présentées ici.

93. - Ainsi de S. Drillon, « La révolution Blockchain », art. préc., qui présente notamment la vulnérabilité connue sous le nom « d'attaque des 51 % » au n° 13.

94. - Y. Cohen-Hadria, « Blockchain... », art. préc. : « (...) la "clé publique" que nous décrivions plus haut est un identifiant personnel qui est conservé de manière à garantir son intégrité. En outre, la clé privée également évoquée supra est une signature électronique au sens de l'article 1367 du code civil. Les données stockées et conservées à travers la chaîne de transaction de type Blockchain sont donc des moyens de preuve électronique aussi forts que des écrits papier ».

95. - Article 1366 du Code civil.

être évité⁹⁶. Mais une fois que cette autorité de certification a confié à chaque citoyen une clé de chiffrement personnelle correspondant à une identité vérifiée, une fois que les joueurs sont connus, la *blockchain* peut arbitrer seule la suite de la partie.

Ainsi, la technologie *blockchain* ne saurait résoudre à elle seule les difficultés suscitées par les concepts de signature électronique et d'écrit électronique, mais son développement fournira sans doute une partie des solutions.

Il reste qu'à l'heure actuelle, la place de l'écrit électronique dans la pratique des contrats en ligne reste tout à fait marginale. Il faut alors se contenter de modes de preuve plus frustes et moins puissants.

2. – La place centrale des modes de preuve imparfaits

283. Cas dans lesquels un écrit est exigé – Admettons qu'en général, le commerçant en ligne ne dispose pas d'un écrit électronique. Dans la grande majorité des transactions passées sur Internet, la valeur en litige est inférieure à 1500 euros, ce qui autorise le recours à des modes de preuve différents⁹⁷. Mis à part l'aveu et le serment judiciaire, qui ont vocation ici comme ailleurs à jouer un rôle extrêmement marginal, il s'agira alors de preuves dites « imparfaites », en ce que leur force de conviction sera librement appréciée par le juge⁹⁸.

Il n'est cependant pas exclu que la valeur en litige soit supérieure à 1500 euros dans le cas d'achats de matériel informatique, photographique, d'électroménager, d'instruments de musique... Là, l'écrit est en principe obligatoire, mais il existe des exceptions.

284. Dérogations – La première exception profite à celui qui peut se prévaloir d'un commencement de preuve par écrit. Il s'agit de « tout écrit qui, émanant de celui qui conteste un acte ou de celui qu'il représente, rend vraisemblable ce qui est allégué » : il sera alors possible

96. - En ce sens, T. Verbiest, « Technologies de registre distribué... », art. préc. : « La question centrale est donc celle de l'identification, sur un réseau qui garantit normalement l'anonymat des parties : celles-ci ne sont "représentées" que par une clé publique. Cette clé n'est pas reliée à une personne physique ou morale pour assurer l'identification de l'auteur de l'acte, comme dans le régime légal de la signature électronique. En effet, pour qu'une signature électronique ait force probante, elle doit bénéficier d'une présomption de fiabilité, laquelle résulte de l'usage d'un procédé d'identification établi grâce à un dispositif sécurisé de création de signature électronique et permettant la vérification de cette signature par l'utilisation d'un certificat électronique délivré par un prestataire qualifié. En d'autres termes, pour qu'un contrat conclu via la *blockchain* soit valable, il faudrait une identification des parties assurée, soit de manière certaine, par une signature électronique "légale" (qui suppose l'intervention d'un tiers de confiance), soit par un autre procédé laissé à l'appréciation du juge ».

97. - Art. 1359 C. civ. *a contrario*. Ainsi qu'il a déjà été rappelé, la preuve sera libre également dans le cas, qui n'est pas celui qui nous intéresse ici au premier chef, d'un client commerçant, et ce quelle que fût la valeur en litige (art. L. 110-3 C. com.).

98. - J.-L. Mouralis, Rép. civ. Dalloz, V° « Preuve (2° règles de preuve », avril 2017, n° 175.

d'avoir recours à tout autre mode de preuve pour compléter, par un élément distinct, ce commencement de preuve par écrit⁹⁹. Ce complément constituera une preuve imparfaite, c'est-à-dire que le juge aura à apprécier sa force de conviction, ce qu'il n'aurait pas eu à faire face à une preuve littérale en bonne et due forme.

Une deuxième exception à l'exigence d'une preuve littérale au-delà de 1500 euros peut être rappelée. L'article 1360 du Code civil prévoit le cas de l'impossibilité matérielle d'établir un écrit à laquelle se serait heurtée la partie qui cherche à prouver l'obligation. Un auteur explique ainsi : « [...] en l'état de la science et de la technique et de l'absence de signature sécurisées au sens strict, il n'est jamais possible d'établir électroniquement une preuve littérale »¹⁰⁰. À supposer que l'argument ait été valable un jour, il semble à présent daté : pour des transactions d'un tel montant, les solutions techniques existent et pourraient être mises en place.

285. **Plan** - Gardons tout de même à l'esprit que la grande masse des transactions en ligne est inférieure au seuil de 1500 euros. Cela explique que l'on se contente de modes de preuve imparfaits. Leur simplicité (a) compense leurs faiblesses (b).

a – Simplicité

286. **Les logs : admissibilité** – Il s'agit de rechercher une trace des connexions ayant mené à la conclusion du contrat dans le journal interne du serveur tenu par le commerçant ou la plateforme. Commençons par souligner qu'un tel document ne peut certainement pas être considéré comme un commencement de preuve par écrit. La définition du Code civil, que nous avons rappelée, précise qu'il doit s'agir d'un écrit émanant de celui qui conteste l'acte. Tel n'est pas le cas document tiré du serveur du commerçant en ligne¹⁰¹. Poursuivons néanmoins notre examen de la valeur probante de ce document, en gardant à l'esprit que, si la valeur en litige est supérieure à 1500 euros, il ne pourra servir que comme complément extrinsèque à une tierce pièce qui, elle, répondrait aux exigences posées pour les commencements de preuve par écrit.

99. - Art. 1362 C. civ.

100. - A. Penneau, « La signature électronique. Rapport de droit français », *RLDI*, 2009, n° 52, supplément spécial, p. 36, n° 19. L'auteur évoque même la possibilité, ouverte par le même texte, d'une impossibilité morale d'établir un écrit, au regard de la jurisprudence de la Cour de cassation « admettant que l'impossibilité morale d'établir un écrit puisse être extirpée d'un usage de ne pas signer un acte » (n° 20). Mais Mme Penneau rejette rapidement cette idée.

101. - En ce sens : À. Hollande, *op. cit.*, n° 1723. Il a ainsi été jugé, dans une hypothèse très proche, que le relevé des communications téléphoniques par France Télécom ne peut valoir commencement de preuve par écrit contre son abonné : Cass. 1ère civ., 12 juill. 2005, pourvoi n° 04-15314 : Bull. civ., I, n° 328 ; CCC, 2006, n° 3, obs. L. Leveneur.

L'ancien article 1349 du Code civil, dont il n'y a plus d'équivalent exact depuis l'ordonnance de 2016, disposait : « Les présomptions sont des conséquences que la loi ou le magistrat tire d'un fait connu à un fait inconnu ». Il existe ainsi des présomptions légales, qui ne nous intéressent pas ici, mais également des « présomptions qui ne sont point établies par la loi »¹⁰², que la doctrine nommait « présomptions du fait de l'homme »¹⁰³. Celles-ci figurent au nouvel article 1382 du même Code : « Les présomptions qui ne sont pas établies par la loi, sont laissées à l'appréciation du juge, qui ne doit les admettre que si elles sont graves, précises et concordantes, et dans les cas seulement où la loi admet la preuve par tout moyen. ». Qu'est-ce qu'un *log*, du point de vue du droit des preuves, si ce n'est une telle présomption¹⁰⁴? D'un fait connu — il existe une trace dans un fichier informatique — le juge va tirer un fait inconnu — cette trace a été créée par l'action du client, souscrivant le contrat électronique.

Néanmoins, on songera peut-être à opposer à la production du *log* l'ancien adage, devenu récemment article de loi : « nul ne peut se constituer de preuve à soi-même (*sic*) »¹⁰⁵. Mais il faut se représenter le sens de cette règle le plus exactement possible, tant il apparaît que les contrats du commerce électronique mettent « le droit de la preuve à l'épreuve de l'unilatéralisme »¹⁰⁶. Or cette sentence est largement critiquée en doctrine, du moins en ce qu'elle prétendrait s'opposer à toute production d'une preuve unilatérale, dans son principe même. Un premier niveau de critique consiste à affirmer que les preuves unilatérales peuvent et doivent être examinées par le juge, mais qu'elles ne peuvent simplement pas suffire, à elles seules, à emporter sa conviction¹⁰⁷. Certains arrêts ont pu sembler en ce sens¹⁰⁸. Un second niveau de critique va jusqu'à prétendre qu'il est possible de convaincre le juge sur la seule foi d'une ou plusieurs preuves unilatérales, si le magistrat en vient à estimer que la manière dont ces preuves ont été constituées mérite sa confiance¹⁰⁹. Ainsi des juges, pour constater que des passagers s'étaient présentés tardivement au comptoir de leur

102. - C'était le titre du paragraphe du Code civil contenant l'article 1353 du Code civil, devenu 1382 depuis l'ordonnance de 2016.

103. - V. J.-L. Mouralis, V° Preuve (1° modes de preuve), in Rép. civ. Dalloz, avril 2017, n° 665 s.

104. - En ce sens, très clairement : A. Hollande, *op. cit.*, n° 1724.

105. - Article 1363 du Code civil, issu de l'ordonnance de 2016.

106. - Cette formule constitue une partie du titre de l'étude approfondie que C. Mouly-Guillemaud a consacré à l'adage : « La sentence "nul ne peut se constituer de preuve à soi-même" ou le droit de la preuve à l'épreuve de l'unilatéralisme », *RTD. civ.*, 2007, p. 253.

107. - V. ainsi, très clairement, D. Gutmann, note ss. Cass. 2e civ., 2 avr. 1996 : *LPA*, 24 janv. 1997, n° 11, p. 19.

108. - Par ex. Cass. 1ère civ., 2 avr. 1996, pourvoi n° 93-17181 : *Bull. civ.*, I, n° 170 ; D. Gutmann, note préc. ; *RTD. civ.*, 1997, p. 136, obs. J. Mestre ; *D.*, 1996, somm., p. 329, obs. P. Delebecque. Cet arrêt reproche à une cour d'appel d'avoir rejeté la demande en indemnisation de la victime d'un accident impliquant un train, « en se fondant **exclusivement** sur des éléments de preuve émanant de la SNCF » (nous soulignons).

109. - En ce sens not., C. Mouly-Guillemaud, art. préc.

compagnie aérienne, se sont-ils reposés sur le seul « listing informatique des opérations d'enregistrement », dans la mesure où une entrée ne peut être apposée sur ce registre sans que ces passagers n'aient présenté leurs documents personnels : c'est la manière dont le procédé est construit qui le rend crédible¹¹⁰. Les relevés des communications par l'opérateur téléphonique, ensuite, constituent une hypothèse plus proche encore de celle qui nous occupe. Nous avons souligné précédemment qu'ils ne peuvent valoir commencement de preuve par écrit, puisqu'ils n'émanent pas de la partie contre laquelle la demande est dirigée. Mais il a été jugé qu'ils peuvent valoir comme présomption, et cette seule présomption peut suffire à emporter la conviction des magistrats¹¹¹.

Il semble donc qu'il ne reste pas grand-chose de l'adage « nul ne peut se constituer... », et que la présomption tirée d'une preuve unilatérale soit finalement une présomption comme une autre¹¹². La preuve unilatérale n'en est pas moins une preuve, lorsqu'elle parvient à convaincre.

287. Les logs : force de conviction - Quelles sont alors les chances que les magistrats soient convaincus par la production des *logs* ? Nécessairement assistés sur ces questions par des experts, les juges auront à examiner la plateforme technique mise en place par le commerçant, et à en apprécier la fiabilité : comment sont conçus les logiciels permettant le fonctionnement du serveur informatique ? Comment construisent-ils le journal des opérations : y a-t-il un risque élevé d'erreur, de falsification ? A-t-on recours à un tiers prestataire, et si oui peut-on en déduire que les données sont dignes d'une plus grande confiance ? À considérer que les différents processus ayant abouti à la production des données produites devant le juge sont tous fiables, on aboutira le plus souvent à un lien entre un panier de produits — biens ou prestations de services — d'une part, et un utilisateur d'autre part. Par « utilisateur » on entend deux types de données : celles qui ont été renseignées dans le compte client, dont on a déjà vu qu'elles étaient purement déclaratives et dont la valeur probatoire est donc très faible, mais aussi les données relatives à l'adresse IP de l'utilisateur. L'adresse IP a déjà été définie plus haut comme un identifiant chiffré, unique, attribué à une machine ou à un ensemble de machines connectées à Internet¹¹³. Si le point d'accès au réseau est un domicile particulier, on ne saura pas pour autant lequel des habitants du domicile, ou des amis de

110. - Cass. 1ère civ., 13 juill. 2004, pourvoi n° 01-11.729 : Bull. civ., I, n° 107 ; *D.*, 2004, p. 2524, note N. Léger.

111. - Cass. 1ère civ., 28 janv. 2003, pourvoi n° 00-17.553 : Bull. civ., I, n° 26 ; *CCE*, 2003, n° 11, p. 37, obs. P. Stoffel-Munck ; *CCC*, 2003, n° 6, p. 15, obs. L. Leveneur.

112. - Dans sa version la plus ancienne, axée sur le mot « *titre* » et non « *preuve* », l'adage signifierait tout de même qu'une preuve unilatérale ne peut valoir preuve littérale (un titre), mais on considérera avec un auteur il n'y a là qu'une « *inutile évidence* » (C. Mouly-Guillemaud, art. préc.).

113. - *V.supra*, n°51.

passage tenait la souris au moment de la commande. Il est également possible qu'un réseau sans fil domestique mal sécurisé soit piraté : l'acheteur réel sera alors masqué derrière l'IP d'un acheteur apparent. D'autre part, l'adresse peut être celle d'un accès collectif, cybercafé ou entreprise, ce qui rend la traque encore plus difficile. Ajoutons que le commerçant dispose de l'adresse IP et de l'heure de la transaction, mais qu'il ne peut en déduire lui-même à qui cette adresse était attribuée : seuls les FAI disposent de cette information, et ils ne la délivrent généralement qu'à la demande de la justice – cette mesure ayant évidemment un coût.

La description qui vient d'être donnée vaut dans le cas d'une commande à partir d'un poste informatique classique. Mais dans le cas d'une commande passée à partir d'un *smartphone*, l'utilisateur relie dès l'acquisition son compte utilisateur à sa carte SIM, c'est-à-dire à un contrat de téléphonie mobile dont le titulaire est, quant à lui, bien identifié, ce qui écarte les difficultés liées à une utilisation collective du terminal. De plus, lors d'un achat d'application ou de contenu via la plateforme intégrée au téléphone, par exemple iTunes (pour Apple) ou Google Play, la tabulation d'un mot de passe personnel est nécessaire¹¹⁴. Les magistrats pourraient peut-être y voir des éléments allant dans le sens d'une fiabilité supérieure¹¹⁵. L'achat de contenu depuis la « box » d'un FAI relie également le mot de passe à une personne physique dont l'identification a été vérifiée (au moment de l'abonnement à Internet)¹¹⁶.

Quoi qu'il en soit, il apparaît que les investigations à réaliser sont complexes, d'une durée et d'un coût qui sont généralement sans rapport avec la valeur en litige, et qu'elles risquent de placer le juge dans les mains des experts informatiques.

114. - Sauf nouvelle commande passée dans les minutes suivant la première, le concepteur présumant que, durant ce court laps de temps, le terminal reste sous le contrôle ou du moins sous la surveillance de son propriétaire

115. - Faut-il aller jusqu'à voir dans ces procédés une forme de signature électronique, puisqu'ici le mot de passe est directement relié à une personne physique identifiée ? Nous ne le croyons pas. Rappelons que la signature électronique « *consiste en l'usage d'un procédé fiable d'identification garantissant son lien avec l'acte auquel elle s'attache* » (art. 1316-4 al. 2 C. civ.). Si l'identification est peut-être ici relativement fiable — la question appartient avant tout aux experts informatiques —, la condition manquante est celle du « *lien avec l'acte* ». La signature électronique « *présumée fiable* » telle que prévue par les décrets mêle en effet, par l'intermédiaire de techniques cryptographiques, la signature et le texte du contrat, en un ensemble unique jusqu'à son déchiffrement. S'il est théoriquement possible, à la lecture du texte, de prévoir un système de signature électronique qui ne soit pas conforme au décret — à charge alors de prouver sa fiabilité — sa physionomie reste encore à définir : comment garantir, autrement que par le système du décret, le lien avec l'acte ? V. sur ce point D. Guinier, « Une signature numérique insatisfaisante est-elle encore une signature ? », *Gaz. Pal.*, 19 avr. 2001, p. 14 et J. Devèze, « Vive l'article 1322 ! Commentaire critique de l'article 1316-4 du Code civil », in *Mélanges Catala*, Litec, 2001, p. 529, spéc. p. 535 s.

116. - En pilotant l'une de ces « box » à l'aide d'une télécommande, et en fournissant un mot de passe défini lors de la souscription de l'abonnement à internet, il est par exemple possible de louer un film pour quelques heures. Il sera téléchargé, diffusé sur la télévision, et facturé. Ce système ne doit pas être confondu avec les dispositifs de type « Internet plus » dont il sera question infra, n°297, par lesquels les fournisseurs d'accès à Internet facturent du contenu vendu par des tiers et non par eux-mêmes.

Heureusement, d'autres éléments pourront alimenter le débat probatoire, au premier rang desquels l'utilisation de moyens de paiement par l'acheteur.

288. Les moyens de paiement - Le client aura nécessairement réglé sa commande au cybermarchand. Les instruments de paiement dont il se sera servi pourront le plus souvent être utilisés par le commerçant pour prouver que le contrat a bien été conclu, et pour identifier son partenaire. Les modes de paiement les plus classiquement employés sont le chèque, le virement, et la carte bancaire.

Un chèque est un ordre de paiement écrit, donné par le client à sa banque, qui permet de l'identifier précisément. Il peut être considéré comme une preuve littérale, et est assorti de la force particulière que lui confère le droit cambiaire : « [...] les effets de commerce représentent toujours une somme d'argent incorporée au titre lui-même, l'autonomie du rapport cambiaire assurant cette incorporation. Il s'ensuit que, contrairement au titre civil pour lequel *l'instrumentum* ne constitue qu'un moyen de preuve, pour les effets [de commerce], le titre incarne le droit lui-même »¹¹⁷. Même lorsque le chèque est irrégulier, parce qu'il ne contient pas les mentions obligatoires, ou que son encaissement est demandé tardivement, il peut encore valoir comme commencement de preuve par écrit¹¹⁸.

Lorsque le commerçant est payé par virement, il ne bénéficie pas, cette fois-ci, d'une preuve littérale parfaite comme dans le cas d'un chèque régulier. En effet, à supposer qu'il existe un ordre de virement écrit et signé — ce qui n'est pas systématique puisque, en tant que mandat, il obéit au principe du consensualisme¹¹⁹ —, ce n'est pas le webmarchand qui est en sa possession, mais la banque. Toutefois, la trace du virement dans les comptes du bénéficiaire peut valoir commencement de preuve par écrit, lorsqu'elle est accompagnée d'un libellé qui fait référence à la prestation contestée¹²⁰. Concourant à la preuve de la créance, le virement peut également concourir à la preuve de l'imputabilité de l'opération : l'identité de son auteur sera connue, et elle aura été vérifiée par la banque.

117. - D. Gibrila, V° « Effets de commerce », in *Rép. com. Dalloz*, janvier 2010, n° 30.

118. - Cass. com., 5 févr. 1991, pourvoi n° 89-16333(chèque périmé) : Bull. civ., IV, n° 54 ; D., 1991, p. 217, obs. M. Cabrillac ; *RTD. civ.*, 1991, p. 749, obs. J. Mestre ; Cass. 1ère civ., 10 mars 1992, 10 mars 1992, pourvoi n° 90-21.074 (chèque non daté) : Bull. civ., I, n° 78 ; D., 1992, p. 337, obs. M. Cabrillac.

119. - R. Bonhomme, V° « Virement », in *Rép. com. Dalloz*, octobre 2014, n° 48.

120. - Par ex. Cass. 1ère civ., 25 juin 2008, pourvoi n° 07-12545, inédit : CCC, nov. 2008, comm. 256, obs. L. Leveneur. Dans cet arrêt, pas moins de 6800 euros étaient réclamés au titre des « *frais de garde* » d'un chien. Les virements libellés « *garde de chien* » ou « *garde Rocco* » ont pu constituer des commencements de preuve par écrit de l'existence de cette créance.

La majeure partie des paiements en ligne est réalisée au moyen d'une carte bancaire. Dans les comptes du commerçant apparaîtra une trace très proche de celle laissée par un virement : dès lors, on voit mal comment refuser à l'une la qualité de commencement de preuve par écrit qui a été reconnue à l'autre. Toutefois, un tel mode de paiement offre une sécurité bien plus faible lorsque seules les informations faciales de la carte sont réclamées, ce qui est très souvent le cas¹²¹. Si son titulaire prétend qu'il y a eu fraude, il ne sera plus possible de considérer automatiquement que le paiement « émane de celui contre lequel on l'allègue », et il n'y aura donc plus commencement de preuve par écrit¹²².

Les instruments de paiement traditionnels bénéficient donc d'un pouvoir identifiant, dont l'intensité varie selon les circonstances. Mais de nouveaux moyens de paiement en ligne sont en train de se développer à grande vitesse. Certains sont conçus pour le règlement de petites sommes : c'est la question des « micropaiements ». Ils se présentent parfois sous la forme d'une créance « au porteur » : chèques cadeaux, identifiants à usage unique... Le paiement est alors entièrement anonyme, qualité qui, loin d'être accidentelle, est au contraire mise en avant par les fournisseurs de ces services¹²³. Il sera alors impossible d'imputer le contrat électronique, de manière fiable, à une personne physique précise, mais tel est également le cas des achats de petits montants réglés en espèces dans le commerce traditionnel. De plus, il est possible pour le vendeur de « monnaie électronique » d'en proposer deux versions, dont l'une est réservée aux mineurs. Si un mineur en fait l'acquisition, ou qu'un adulte déclare acheter cette monnaie pour l'offrir à un mineur, le code identifiant qui sera délivré ne permettra pas l'achat de certains produits réservés à un public de majeurs¹²⁴.

Un problème similaire est posé par l'utilisation de monnaies électroniques de type bitcoins¹²⁵. Ainsi qu'il a été exposé, la circulation de cette devise virtuelle est retranscrite dans un registre fondé sur la technologie des chaînes de blocs, qui n'impose nullement dans son principe que ses utilisateurs fournissent une identité réelle et vérifiée. Accepter des paiements en bitcoins revient

121. - Pas toujours, puisque certains systèmes de paiement par carte bancaire réclament en outre que soit saisie la date de naissance du titulaire de la carte, voire un code de sécurité envoyé sur son téléphone portable : V.infra, n°295.

122. - Pour trancher cette question, il faudra donc au préalable déterminer si la fraude dénoncée a réellement eu lieu.

123. - C'était le cas du service Wexpay, qui proposait d'acheter des identifiants à usage unique, d'une valeur libératoire comprise entre 5 et 250 euros, par exemple chez un buraliste. La société a cependant récemment cessé ses activités.

124. - Wexpay proposait ainsi un système baptisé « contrôle parental de paiement ».

125. - Pour un aperçu général, V. par ex. C. Laverdet, « Bitcoins et autres cryptomonnaies : enjeux et défis juridiques », in *Les biens numériques*, éd. Ceprisca, 2015, p. 33.

donc à accepter le principe d'une clientèle d'anonymes. Les motifs peuvent être louables — afficher une politique rassurante en matière de collecte de données personnelles — ou plus douteux — proposer des biens et services illicites¹²⁶. Précisons cependant que les services de l'État, qu'il s'agisse de l'administration fiscale ou de la police, ne sont pas dénués de tout moyen d'investigation permettant de mettre au jour les identités réelles cachées derrière les comptes en cryptomonnaies¹²⁷.

289. Les justificatifs de domicile ou d'identité - Afin de combattre les détournements de moyens de paiement et les usurpations d'identité, dont nous avons vu qu'ils étaient rendus plus aisés par les systèmes de vente à distance, certains commerçants avertissent leur clientèle qu'ils sont susceptibles de réclamer des documents supplémentaires s'ils le jugent utile. Ainsi, les conditions générales de Rue du commerce contiennent-elles l'article suivant : « 3.2. Les contrôles anti-fraude. Afin d'assurer la sécurité des transactions et de répondre au souci du plus grand nombre de prévenir les fraudes en matière de vente à distance, nous effectuons des contrôles sur la passation des commandes. Dans le cadre d'un contrôle, nous vous invitons par courriel à transmettre des justificatifs de domicile et d'identité (le but étant de s'assurer de la réalité de l'identité et de la domiciliation (par exemple une quittance d'électricité, une facture de téléphone fixe pour la perfection de la commande) [...] »¹²⁸.

De tels documents, au contenu neutre, peuvent difficilement être considérés comme « rendant vraisemblable » la volonté de passer une transaction précise : par conséquent, ils ne paraissent pas devoir être considérés comme des commencements de preuve par écrit. Le juge pourrait cependant y voir de simples présomptions, concourant à la démonstration qu'il n'y a eu aucune usurpation d'identité, et que les autres preuves présentées — log, trace d'un paiement — émanaient bien de l'acheteur apparent. Mais il semble évident que les enseignes recueillant ces documents ne cherchent pas à se constituer des preuves susceptibles d'être présentées lors d'un contentieux : il s'agit d'une démarche essentiellement préventive.

290. Le rôle éventuel des conventions de preuve - Les règles du droit probatoire ne sont pas toujours impératives. En effet, s'agissant des droits « dont les parties ont la libre disposition, [les] conventions de preuve sont licites », d'après la jurisprudence¹²⁹. N'est-ce pas la solution parfaite

126. - Pour un exemple relevant de la première catégorie, V. la possibilité de s'abonner au journal d'actualités du numérique Nextinact en réglant en bitcoins (<https://www.nextinact.com/blog/93538-le-paiement-par-bitcoin-est-disponible-pour-nos-abonnements.htm>). Pour des exemples relevant de la seconde catégorie, V. par ex. O. de Maison Rouge, « Darkweb : plongée en eaux troubles », *Dalloz IP/IT*, p. 74.

127. - V. par ex. V. Charpiat, « Le bitcoin devient monnaie courante : les monnaies digitales entre transparence et innovation », *Revue des Juristes de Sciences Po*, n° 9, juin 2014.

128. - Conditions générales consultables sur www.rueducommerce.fr, datées du 21 avril 2017 et encore en vigueur en septembre 2017.

129. - Cass. 1ère civ. 8 nov. 1989, *Crédicas*, pourvois n° 86-16196 et 86-16197 : Bull. civ., I, n° 342.

aux problèmes soulevés jusqu'ici ? Ce n'est pas aussi évident, et les observations qui vont suivre appellent à la prudence.

Tout d'abord, il faut que la convention déroge suffisamment clairement aux règles légales de preuve. À cet égard, une ancienne version des conditions générales des magasins en ligne d'Apple (les Stores), constituait un contre-exemple intéressant : « L'utilisation des Stores vous donne la possibilité de conclure des contrats et/ou d'effectuer des transactions électroniquement. Vous reconnaissez que vos demandes électroniques constituent votre accord et votre volonté d'être lié contractuellement et de payer pour ces contrats et achats. [...] »¹³⁰. On voit mal ce qu'apporte une telle stipulation. Est tout à fait claire, en revanche, la clause des conditions générales de la FNAC relative au téléchargement de livres numériques, ainsi libellée (art. 3) : « [...] Sauf preuve contraire, les données enregistrées par Fnac Direct constituent la preuve de l'ensemble des transactions passées par Fnac Direct et ses clients »¹³¹.

Ensuite, les auteurs s'accordent à dire que la convention de preuve ne peut faire davantage que poser une présomption simple, qui doit pouvoir être renversée¹³² – c'est le cas dans les conditions générales FNAC précitées. En pratique, est-il vraiment possible pour le client d'apporter la preuve contraire ? De plus, même si l'on s'en tient à une présomption simple, ne confère-t-on pas *in fine* aux logs des serveurs de la FNAC la même valeur probante qu'une véritable signature électronique fiable, au sens du Code civil et de ses décrets d'application ? Rappelons en effet que le respect des sévères exigences de ces textes ne vaut que présomption simple de fiabilité du procédé¹³³. Il suffirait alors de faire de cette convention de preuve une clause de style dans les conditions générales des cybermarchands pour contourner complètement la « forteresse » de la signature électronique, en donnant à une simple preuve unilatérale la même valeur : tout ça pour ça¹³⁴ ?

Mais une dernière remarque, plus fondamentale, vient jeter le doute sur la possibilité même de stipuler de telles conventions sur la preuve. Dans le cas de contrats isolés, survient en effet une

130. - Conditions générales des App Store, version du 6 décembre 2012.

131. - Conditions générales consultables sur http://multimedia.fnac.com/multimedia/fnacdirect/pdf/cgv/Conditions_Generales_de_Telechargement_Livre_Numerique_14102014.pdf, version du 14 octobre 2014.

132. - En ce sens : L. Grynbaum, « La preuve littérale... », art. préc., n° 36. Rappr. art. R. 132-2, 9° C. conso., qui prohibe comme abusives ayant pour objet ou pour effet de « limiter indûment les moyens de preuve à la disposition du non-professionnel ou du consommateur ».

133. - Que reste-t-il alors des préoccupations de la Commission des clauses abusives (supra, n° 280), selon lesquelles on faisait parfois croire au client que le double-clic a la même valeur probatoire qu'une véritable signature électronique ? N'est-ce pas nécessairement le cas, dès lors qu'il y a convention de preuve ?

134. - La preuve contraire à rapporter par le client semble la même dans les deux cas : démontrer que la trace électronique qu'on lui oppose n'est pas fiable.

impossibilité logique d'en tenir quelque compte que ce soit. L'utilisation traditionnelle de ce procédé par les banques repose sur un montage solide : les conditions générales d'utilisation des cartes bancaires sont signées en agence, sur un contrat « papier », et posent par exemple que, pour l'avenir, la tabulation du code PIN, ou plus précisément sa trace dans les serveurs de la banque, vaudra comme preuve entre les parties. Mais si l'on passe un seul contrat électronique ponctuel, le système ne fonctionne plus ! Pour prouver qu'un contrat a été passé, on ne peut se référer à une convention de preuve figurant dans ledit contrat, car elle ne pourra produire ses effets que... s'il est prouvé qu'elle a été acceptée : c'est une boucle de raisonnement. Le mécanisme n'a donc d'intérêt que s'il figure dans un premier contrat-cadre dont l'assise probatoire est, quant à elle, d'une solidité incontestable au regard des règles légales. Ce n'est qu'ainsi qu'il sera possible de changer les règles du jeu : pour l'avenir seulement¹³⁵.

De l'ensemble de ce qui précède, il résulte que les moyens de preuve que l'on aurait cru *a priori* incontournables en la matière — preuve littérale électronique et convention de preuve — se sont révélés d'un usage extrêmement minoritaire, presque anecdotique. Ce sont des concepts anciens du droit probatoire qui sont mobilisés : les commencements de preuve par écrit, et les présomptions du fait de l'homme. De plus, les *logs* tirés des serveurs du marchand ne sont destinés, la plupart du temps, qu'à jouer un rôle accessoire, à côté de la preuve plus fiable et plus précise que constitue le moyen de paiement. Les failles d'un tel système sont nombreuses.

b – Faiblesses

291. **Quels risques ?** - Au regard des éléments théoriques qui ont été réunis, il faut à présent se demander si le système probatoire français fonctionne de manière satisfaisante en pratique. L'absence de contentieux notable en la matière ne suffit pas à se réjouir en effet : elle pourrait s'expliquer, bien souvent, par la relative faiblesse des valeurs en litige, de nature à dissuader une partie d'agir quand bien même elle s'estimerait lésée.

Quels sont les risques qu'un acheteur utilise les règles du droit probatoire pour revenir, de mauvaise foi, sur un engagement qu'il aurait pourtant bel et bien pris ? Tout d'abord, s'il est un consommateur, relevons qu'il dispose en matière de vente ou de prestation de service conclue à distance d'un droit de rétractation¹³⁶ : s'il regrette son achat, il n'aura pas besoin de se placer, de mauvaise foi, sur le terrain probatoire. Ensuite, il aura été identifié par son paiement. Mais nous

135. - *Contra* C. Castets-Renard, *Droit de l'Internet...*, *op. cit.*, n° 424, qui, après avoir évoqué la possibilité de conclure des conventions sur la preuve, conclut à son utilité : « L'usage d'un dispositif de signature électronique pour le commerce électronique n'est donc pas nécessaire ».

136. - Art. L. 221-18 C. conso. Certaines exceptions sont cependant prévues par les textes.

avons vu que le paiement par carte bancaire est le plus fréquent, et qu'il est souvent réalisé par simple indication des numéros figurant au recto et au verso de la carte. En raison du risque élevé de fraude qui résulte d'un tel système, le Code monétaire et financier a mis en place un système d'indemnisation¹³⁷. Il suffit pour l'essentiel d'une simple déclaration du titulaire du moyen de paiement, selon laquelle il n'a pas autorisé la transaction, pour que l'établissement de crédit soit amené à le rembourser intégralement, se retournant ensuite contre le marchand¹³⁸. Mais, dans un second temps, le vendeur pourrait utiliser les autres preuves dont il dispose pour conforter celle qui résulte du paiement par carte bancaire : enregistrement de la transaction dans les *logs* de ses serveurs, présomption découlant de l'adresse de livraison si elle correspond au domicile du titulaire de la carte et même, si la valeur de la transaction était importante, justificatifs d'identité ou de domicile que l'on n'aura pas manqué de lui réclamer. Fort de ces présomptions concordantes, le marchand pourrait tenter de prouver l'existence du contrat, et en réclamer l'exécution forcée, ce qui contraindrait le client à payer à nouveau¹³⁹. Nous verrons toutefois qu'il pourrait être difficile de convaincre le juge, tant il sera parfois délicat de distinguer ces indices de ceux résultant d'une situation dans laquelle la carte a bien été volée, en particulier si l'acheteur a fourni une adresse postale qui n'est pas la sienne ni celle d'un proche.

Les situations les plus préoccupantes, précisément, sont celles qui tiennent à l'intervention d'une tierce personne, qui interpose entre elle et le marchand un acheteur apparent, pour mieux se livrer à une forme de fraude. Les délinquants n'ont évidemment pas attendu le numérique pour traquer les failles des circuits commerçants, en tâchant d'en tirer parti. Mais le commerce électronique offre de nouvelles vulnérabilités, susceptibles d'être exploitées à grande échelle. La fraude repose presque toujours sur un numéro de carte bancaire volé, et sur le système déjà décrit qui permet de payer à l'aide de ces seules informations. On parle de « deux fraudes à la minute pour les achats par carte bancaire sur Internet »¹⁴⁰. Cette fraude est particulièrement redoutable lorsqu'elle relève d'une forme de crime organisé : elle tend à concerner des montants de plus en plus considérables (alpha).

137. - Art. L. 133-18 et s. CMF, notamment l'art. L. 133-19, I dans le cas d'un paiement effectué sans dispositif de sécurité personnalisé. *Adde* l'art. 15 du contrat-type carte bancaire. Sur cette question, V. J. Lasserre-Capdeville, « Le droit régissant le paiement par Internet en France », *RLDA*, 2012, n° 73, p. 84.

138. - Ce recours des établissements bancaires contre les marchands est systématiquement prévu par les conventions passées entre eux.

139. - Une qualification pénale pourra également être envisagée, qui dépendra des circonstances précises du mensonge.

140. - C'est le titre d'un article du journal *Le Monde* du 16 février 2012, mis à jour le 26 septembre 2012 sur www.lemonde.fr. *Adde* les chiffres de l'Observatoire de la sécurité des cartes de paiement, consultables sur <http://www.banque-france.fr/observatoire/home.htm>. Le rapport annuel 2011 précise : « [...] seulement 23 % des transactions de paiement sur Internet sont sécurisées par des dispositifs d'authentification non rejouable [...] ». Sur ces dispositifs, V.infra, n°295.

Mais un autre phénomène, que la pratique a pris l'habitude d'appeler « fraude familiale », mérite que l'on s'y arrête, quoique ses enjeux semblent moindres (bêta).

Alpha – La fraude criminelle

292. **Fraude « simple »** - Le procédé criminel le plus rudimentaire consiste à acheter un maximum d'objets destinés à une revente « au noir » à l'aide de ces cartes, avant que leur titulaire réel ne fasse opposition¹⁴¹. Le mécanisme d'indemnisation issu du Code monétaire et financier, décrit plus haut, aboutira à ce que le client de la banque soit indemnisé par son établissement, puis que l'établissement fasse finalement supporter la perte par le marchand. Ledit marchand pensera peut-être disposer de plusieurs éléments probants contre le client apparent, mais l'analyse révèle leur fragilité. Le moyen de paiement ? Mais son titulaire prétend que le numéro a été volé. Les *logs* du serveur ? Mais ils ne pointeront généralement pas vers l'accès personnel du client apparent à son domicile. Cela pourrait vouloir dire que le client a passé la commande depuis un autre lieu — il peut cliquer depuis n'importe quel accès au réseau, partout dans le monde -, mais cela pourrait aussi signifier que ce n'était pas lui qui agissait. L'adresse de livraison ? Elle correspondra à un nom et à un lieu qui n'ont aucun rapport avec le client apparent. Une enquête de police révélera certainement, ultérieurement, que ce client apparent n'a effectivement rien à voir avec la commande¹⁴². En attendant, le juge civil devrait se montrer extrêmement prudent face à une demande d'exécution forcée : son pouvoir de libre appréciation des présomptions devrait être exercé avec tact et mesure.

Que peuvent faire les marchands ? D'abord, mettre en place des techniques statistiques révélant la probabilité de fraude pour une commande donnée : en fonction du lieu de connexion, du type d'adresse de livraison, du profil de la commande, des « matrices de risque » sont construites, qui appellent une intervention humaine pour que la commande soit validée et livrée. Des justificatifs de domicile ou d'identité sont alors réclamés par les préposés du commerçant, ou même une image scannée de la carte bancaire — cryptogramme masqué — afin de démontrer que celui qui commande en possède la maîtrise physique, et qu'il n'a pas seulement recopié les numéros. Mais de tels justificatifs peuvent être falsifiés par des graphistes bien formés. De plus, une nouvelle forme de fraude s'est développée en réaction à ces exigences de justificatifs.

141. - L'ensemble des phénomènes de fraude ici décrits a été découvert par l'auteur à l'occasion d'un entretien avec M. Christophe Davy, dirigeant d'une PME du commerce électronique d'articles de luxes, à lire en annexe de notre étude précitée « Réflexions sur la preuve... ».

142. - Les marchands ont l'habitude de porter plainte de manière systématique lorsqu'ils sont confrontés à des cartes bancaires volées : V. notre entretien avec M. Christophe Davy.

293. **Fraude « au consignataire »** - Cette technique, appelée par la pratique « fraude au consignataire », repose sur le montage suivant. Des personnes crédules seront recrutées par la voie de petites annonces alléchantes, leur proposant une rémunération mensuelle confortable en contrepartie d'une tâche simple : recevoir chez elles et réexpédier des colis en grand nombre. Ainsi, le fraudeur va pouvoir utiliser l'adresse, les justificatifs d'identité et de domicile du « consignataire » lorsqu'il achètera des biens en réglant avec un numéro de carte bancaire volé. Au bout de quelques semaines, le consignataire, qui ne voit arriver aucune rémunération, s'en inquiète auprès de son « employeur », mais ne reçoit pas de réponse : le fraudeur aura changé de mule entre-temps. Le naïf recevra cependant bien vite la visite des services de police, puisqu'il apparaît comme destinataire de nombreux achats réglés par des moyens de paiement volés. Le fraudeur intelligent ne sera vraisemblablement jamais retrouvé. Les marchands floués disposent-ils d'un fondement leur permettant de se retourner contre le consignataire ? S'ils cherchaient à le désigner comme leur cocontractant réel, mettant en avant l'adresse de livraison et les justificatifs d'identité et de domicile reçus, le consignataire démontrerait au juge que ces présomptions ne doivent pas emporter sa conviction. Il produirait le « contrat de travail » qu'il avait reçu, et arguerait de ce que les commandes étaient en réalité passées par son « commettant ». Mais alors, si le consignataire n'est pas son cocontractant, le marchand pourrait tenter d'engager sa responsabilité civile délictuelle : en acceptant de se prêter à ces opérations de réexpédition de colis pourtant fort suspectes, le consignataire n'a-t-il pas commis la faute d'imprudence prévue à l'article 1241 du Code civil causant par là un préjudice à autrui ? Il faut cependant garder à l'esprit la fameuse jurisprudence Costedoat, selon laquelle : « n'engage pas sa responsabilité à l'égard des tiers le préposé qui agit sans excéder les limites de la mission qui lui a été impartie par son commettant »¹⁴³. Or, même si son salaire ne lui sera jamais versé, le naïf s'est bien placé en situation de subordination, dans le cadre de ce qu'il pensait être un contrat de travail, et croyait accomplir strictement la mission qu'il lui avait été confiée. L'immunité du préposé ne semble devoir céder qu'en cas d'infraction pénale ; la relative imprécision de la jurisprudence en la matière ne permettant pas de déterminer clairement si cette infraction pénale doit être intentionnelle¹⁴⁴, ou si n'importe quelle infraction pénale est suffisante¹⁴⁵. Mais même pour le cas où une simple infraction pénale non intentionnelle suffirait, il

143. - Cass., ass. plén., 25 févr. 2000, n° 97-17.387 et 97-20.152 : *Bull. ass. plén.*, n° 2 ; *JCP G*, 2000, I, 241, obs. G. Viney et II, 10295, rapp. R. Kessous et note M. Billiau ; *D.*, 2000, p. 673, note P. Brun ; *Dr. et Patr.*, 2000, n° 82, p. 107, obs. F. Chabas ; *RTD. civ.*, 2000, p. 582, obs. P. Jourdain.

144. - En ce sens, V. not. le fameux arrêt *Cousin*, Cass. ass. plén., 14 déc. 2001, n° 00-82.066 : *Bull. ass. plén.*, n° 2 ; *D.*, 2002, 1230, note J. Julien ; *D.* 2002, Somm., 1317, obs. D. Mazeaud ; *JCP G*, 2002, II, 10026, note M. Billiau ; *RTD civ.*, 2002, 109, obs. P. Jourdain.

145. - « Attendu que n'engage pas sa responsabilité à l'égard des tiers, le préposé qui agit sans excéder les limites de la mission qui lui est impartie par son commettant, hors le cas où le préjudice de la victime résulte d'une infraction pénale ou d'une faute intentionnelle » (nous soulignons). Cass. 2e civ., 21 févr. 2008, n° 06-

sera malaisé de trouver une norme pénale que le consignataire aurait violée, lorsqu'il a été authentiquement candide – et le doute sur ce point lui profitera. Le commettant ayant disparu, la victime se retrouve abandonnée à son sort : c'est précisément ce que certains reprochent à la jurisprudence Costedoat¹⁴⁶.

294. **Fraude de type « marketplace »** - Une troisième technique de fraude, plus habile encore, peut être ici décrite. Certaines plateformes de commerce électronique vendent non seulement des produits en leur propre nom, mais jouent encore le rôle d'intermédiaires pour le compte de plus petits commerçants, qui veulent disposer de la visibilité que confère le site d'un des champions du secteur – un service que la pratique nomme *marketplace*. L'internaute qui cherche un article sur le site de la Fnac ou d'Amazon, par exemple, pourra choisir d'acheter ce produit « vendu et expédié » par cette grande marque, ou bien vendu par une plus petite boutique, mais expédié par la grande marque, ou encore vendu et expédié par la petite boutique, pour autant de prix différents. Pour ajouter encore à la confusion, il arrive que le marchand sous-traite la partie logistique à un concurrent sans même l'annoncer à l'internaute. Le résultat est que les internautes ne s'étonnent plus guère de recevoir leurs commandes sous des emballages portant des marques avec lesquelles ils n'avaient pas contracté. Cette faille est exploitée par les fraudeurs. Ils vont proposer à la vente sur une *marketplace* des articles qu'ils ne possèdent pas. Des clients honnêtes vont se présenter pour acheter, et les payer. Les fraudeurs vont encaisser l'argent, puis commander eux-mêmes les articles attendus auprès d'un véritable marchand, mais en payant avec une carte volée. Ils rempliront le bon de commande avec les coordonnées des clients honnêtes, et leur adresse de livraison. Quand ces articles seront présentés à la livraison, les clients vont les accepter en toute bonne foi. Les fraudeurs disparaîtront avec leur argent. Enfin, les marchands payés avec les cartes bancaires volées vont se présenter chez les clients honnêtes, en les accusant de fraude. Le résultat est redoutable : contrairement au naïf consignataire étudié précédemment, le client n'avait quasiment aucun moyen de se douter qu'il était l'instrument d'une mafia. Ici encore, le juge ne devra pas tirer de conclusions trop hâtives des présomptions dont il dispose — adresse de livraison, fait que la commande a été acceptée, la chose déballée et utilisée — car les apparences sont entièrement trompeuses. Rétablir le véritable scénario qui s'est déroulé interdit au marchand de considérer celui qu'il a livré comme son cocontractant et donc de lui réclamer paiement. Mais, corrélativement, le client devra restituer une

21.182, inédit : RCA 2008, n° 124 ; D., 2008, 2125, note J.-B. Laydu ; JCP G, 2008, I, 186, n° 5, obs. P. Stoffel-Munck.

146. - V. par ex. J. Julien, V° « Responsabilité du fait d'autrui », in *Rép. civ. Dalloz*, juin 2016, n° 145, et les réf. citées.

marchandise qui ne lui appartient pas, et porter plainte pour escroquerie contre le fraudeur qui l'a déterminé à payer par ses manœuvres frauduleuses¹⁴⁷.

De manière générale, dans ces hypothèses de fraude mafieuse, l'aspect pénal ne saurait être négligé : si des poursuites sont engagées, la règle selon laquelle « le pénal tient le civil en l'état » pourrait obliger le juge civil à sursoir à statuer, et à tenir compte des conclusions d'une instance qui aura obéi aux règles de la procédure pénale¹⁴⁸.

295. **Renforcer les systèmes d'authentification** - Les dommages subis par les marchands dans le cadre de ces fraudes pourraient être absorbés par la mise en œuvre d'un mécanisme assurantiel, et le sont déjà certainement très souvent en pratique. Mais, bien évidemment, les coûts afférents à cette couverture sont répercutés sur toutes les transactions « honnêtes » : il est donc fondamental d'éviter que ces phénomènes ne prennent une trop grande ampleur. La solution passe par l'abandon total des possibilités de payer par simple utilisation des données faciales des cartes bancaires : c'est le maillon faible qui rend ces différentes fraudes possibles, et il faut à présent se tourner vers des procédures plus sécurisées¹⁴⁹. Le dispositif « 3d secure », qui tend enfin à se répandre, demande par exemple au client de confirmer le paiement à l'aide d'un code unique reçu par SMS sur son téléphone portable¹⁵⁰. Cette procédure, qui rend la fraude très difficile, tarde à se généraliser parce que, mal connue et mal comprise des clients, elle les dissuadait de poursuivre leur commande, et faisait s'effondrer les transactions pour les sites qui la mettaient en place¹⁵¹. Il est temps de faire évoluer les mentalités. Lorsqu'un tel système de sécurité personnalisé est à l'oeuvre, le Code monétaire et financier précise que le client doit supporter les pertes liées à l'utilisation frauduleuse,

147. - Art. 313-1 C. pén.

148. - Encore faut-il noter que l'article 4 du Code de procédure pénale, qui pose cette solution, a vu son champ d'application nettement restreint par la loi n°2007-291 du 5 mars 2007. Seules les actions civiles menées « *en réparation du dommage* » causé par l'infraction pénale sont paralysées. Dans l'exemple qui vient d'être développé, cela n'empêcherait donc pas une action du marchand en exécution forcée du contrat contre celui qu'il croit être son client : il appartiendrait donc bien au juge civil de repousser cette action, après avoir considéré la faiblesse des présomptions apportées à son soutien, et les doutes suscités par la version exposée par le client victime de la fraude.

149. - C'était notamment l'objet du « Colloque sur la sécurisation des paiements par carte dans un environnement de vente à distance » organisé par la FEVAD le 12 novembre 2012, et réunissant juristes et banquiers, sous l'égide de la ministre déléguée à l'économie numérique de l'époque, Mme Fleur Pellerin.

150. - Plus précisément, la formalité supplémentaire à accomplir dépend de la banque du titulaire du moyen de paiement (V. les différents sites internet des établissements). Il s'agit parfois simplement d'indiquer la date de naissance du titulaire, ou son code postal, ce qui ne procure qu'une très faible sécurité, étant donné la facilité avec laquelle cette information peut être découverte par un fraudeur. D'autres établissements remettent à leurs clients une grille de 64 codes, le client devant saisir à chaque transaction celui qui figure précisément à l'intersection de telle ligne et de telle colonne. D'autres encore demandent la tabulation d'un mot de passe personnel. Le système du code unique envoyé par SMS tend cependant à devenir majoritaire.

151. - V. notre entretien avec M. Christophe Davy en marge de l'article précité « Réflexions sur la preuve et l'imputabilité des contrats électroniques ».

dans la limite de 150 euros¹⁵². De plus, et selon les contrats passés entre les marchands et les établissements bancaires, il arrive que ces derniers prennent le risque à leur charge, pour le surplus, alors que nous avons vu qu'ils le font peser sur le commerçant lorsque le paiement a lieu par simple fourniture des informations faciales de la carte.

Envisageons à présent une forme de fraude moins inquiétante, mais bien réelle : la fraude dite « familiale ».

Bêta – La fraude familiale

296. **Concept** - Ce que les professionnels appellent « fraude familiale » consiste tout simplement dans le détournement des moyens de paiement d'une personne par ses proches, le plus souvent par ses enfants, qui profitent des facilités que leur procure leur présence physique au sein du foyer¹⁵³. Quoi de plus facile, en effet, que de profiter d'une courte absence ou de quelques minutes d'inattention parentale pour recopier les données faciales d'une carte bancaire ? Nous avons vu que ces informations sont généralement suffisantes pour procéder au paiement. Mais un certain système de micropaiement rend la fraude familiale encore plus simple. Le paiement par un jeune enfant pourrait même être involontaire, ou en tout cas inconscient, tandis que l'utilisation de la carte bancaire parentale est toujours une démarche consciente.

297. **Système « Internet plus »** - « Internet plus » est en effet un système de paiement par simple ajout du prix du bien ou du service à la prochaine facture du FAI ou de l'opérateur de téléphonie mobile¹⁵⁴. Ces professionnels de l'accès au réseau se sont regroupés au sein d'une « Association française du multimédia mobile », qui propose des contrats aux fournisseurs de contenu numérique. Ce contenu consiste par exemple en l'accès à un article de journal, l'achat de l'extrait k-bis d'une entreprise, le téléchargement de fonds d'écran ou de sonneries pour téléphones portables... L'idée est la suivante : le FAI facturera et fera payer le service à son abonné, pour le compte du fournisseur de contenu, via un système très efficace. L'internaute n'aura, explique l'association, que « deux clics » à faire pour payer, sans créer aucun compte utilisateur, ni rentrer

152. - Art. L. 133-19 CMF. En effet, cette « franchise » n'est écartée que s'il y a eu paiement « sans utilisation du dispositif de sécurité personnalisé ». Un auteur estime que le système « 3D secure » peut être assimilé à un tel dispositif : J. Lasserre-Capdeville, art. préc., n° 26. Il nous semble que cela n'est vrai que pour les systèmes d'authentification suffisamment forts au sein de l'ensemble appelé « 3D secure ». Tel ne devrait pas être le cas, par exemple, de la saisie de la date de naissance du client.

153. - V. par ex. <http://www.ziserman.com/blog/2010/07/12/la-fraude-familiale-la-fraude-qui-coute-le-plus/>.

154. - <http://internetplus.fr>. Nous développerons ici le cas du système de paiement lié à la facture Internet, qui présente nous semble-t-il davantage de risques de détournement que le système lié au téléphone mobile.

aucun identifiant ou mot de passe. Il est identifié automatiquement, et sa facture Internet est automatiquement débitée du montant correspondant.

Plus précisément, la procédure varie selon l'opérateur : l'identifiant et le mot de passe de l'abonné doivent tout de même être saisis systématiquement chez SFR ; chez Bouygues Telecom, pour le premier achat seulement, s'il est supérieur à 10 euros ; chez Free, pour le premier achat uniquement. Mais chez l'opérateur historique, le système est proposé dans sa version la plus « pure » : le fameux « double clic » exigé par le Code civil – le premier pour accéder à un récapitulatif, le second pour valider le panier – vaut non seulement acceptation du contrat, mais surtout paiement : la somme apparaitra sur la prochaine facture, et sera bien souvent payée par l'abonné sans aucune intervention de sa part, par le simple jeu du prélèvement automatique. Comment est-ce techniquement possible ? Le poste informatique utilisé se connecte au réseau par l'intermédiaire d'un abonnement nominatif, auquel est associé une adresse IP unique, qui sera reconnue et permettra le paiement par simple clic. On aura compris que n'importe quel ordinateur connecté via l'accès Internet familial permettra le paiement, peu importe qui l'utilise.

Afin de mieux apprécier l'innocuité ou les dangers du système, précisons que le montant mensuel total des achats par ce moyen est normalement plafonné à 60 euros¹⁵⁵. La plupart du temps, les petits contenus numériques concernés sont facturés quelques dizaines de centimes, mais le prix unitaire peut aller jusqu'à 30 euros, et il est possible de souscrire un abonnement hebdomadaire pour un prix allant jusqu'à 5 euros¹⁵⁶.

298. Dangers pour les mineurs - Du point de vue des éditeurs de contenus, un tel système est très séduisant, puisqu'il maximise le « taux de conversion », c'est-à-dire l'aptitude d'un site marchand à transformer un visiteur en client payant¹⁵⁷. Du point de vue des clients, corrélativement, le système ne semble pas sans danger. Certains vendeurs de contenus tentent de rendre les mentions relatives au paiement les plus discrètes possible, ce qui se révèle certainement très efficace lorsque c'est un enfant ou un jeune adolescent qui est aux commandes de l'ordinateur. Les FAI ont réagi, en incorporant aux contrats qu'ils passent avec les éditeurs de contenus des « chartes » ou « recommandations déontologiques »¹⁵⁸. Puisqu'il y est renvoyé au sein des conventions passées

155. - C'est en tout cas le chiffre retenu chez Orange : https://assistance.orange.fr/ordinateurs-peripheriques/installer-et-utiliser/un-service-d-orange/les-achats-en-ligne/internet/internet-personnaliser-un-montant-maximum-d-achat_130042-40575.

156. - <http://internetplus.fr>, « espace éditeurs », rubrique « généralités ». Le danger est alors l'accumulation de « micro prélèvements » avant que le titulaire de l'abonnement ne s'aperçoive qu'un service lui est facturé.

157. - C'est ce même indicateur qui avait chuté chez plusieurs commerçants lorsqu'ils avaient mis en place le système 3D secure alors qu'il n'était pas encore suffisamment connu du public.

158. - <http://internetplus.fr>, « espace éditeurs », « déontologie ». Sur cette page, on découvre que des

entre les FAI et les fournisseurs de contenu, ces documents acquièrent, en dépit de leur dénomination, une valeur contractuelle obligatoire. Or, ils prévoient un principe de « loyauté à l'égard des utilisateurs », qui prescrit une transparence tarifaire, et ils posent des règles de forme précises s'agissant de la présentation des offres (choix des polices d'écriture, couleur, taille...). Il nous est cependant arrivé de découvrir des sites dont la présentation dérogeait assez nettement à ces principes, par exemple en marquant en très gros caractères qu'un téléchargement de sonnerie pour téléphone mobile était à zéro euro, et en très petits caractères qu'il s'agissait d'un abonnement facturé 5 euros par semaine, dont seule la première semaine était gratuite¹⁵⁹.

Quand bien même les règles formelles de présentation des offres seraient parfaitement respectées, le risque de dérapage semble réel lorsque le public visé est particulièrement jeune. Le quotidien régional Le Télégramme relate une histoire édifiante de ce point de vue¹⁶⁰. Elle concerne Habbo Hotel, un jeu en ligne prisé des adolescents, basé sur le modèle économique du *free-to-play*, précédemment décrit : l'utilisation est gratuite, mais des options payantes augmentant l'agrément de jeu sont proposées ; elles peuvent être réglées via « Internet plus »¹⁶¹. Cela n'avait pas échappé à deux garçons de 9 et 12 ans, qui ont utilisé l'abonnement de la Maison des jeunes de Questembert, dans le Morbihan, pour s'acheter progressivement 600 euros de « mobilier virtuel » pour décorer leur univers de jeu¹⁶². L'éditeur du jeu a réagi, et les mentions d'avertissement destinées à son jeune public ont été clarifiées¹⁶³. Malgré cela, il est difficile d'affirmer qu'elles parviendront à éclairer suffisamment le consentement d'enfants dont la conception de l'argent, avant un certain âge, est probablement confondue avec la seule figure de la monnaie fiduciaire, celle des pièces et des billets. L'idée qu'on peut dépenser une valeur correspondant à plusieurs dizaines d'euros en deux clics et sans autre formalité requiert certainement une maturité et une capacité à l'abstraction dont tous ne disposent pas ; il faut craindre en tout cas que ces aptitudes ne soient acquises plus tard que l'habileté à manier la souris.

« Commissions déontologiques » ont été créées, et se réunissent régulièrement pour tenter d'imposer de bonnes pratiques.

159. - Il n'est pas possible de donner d'adresse pour exemple, les sites affichant de mauvaises pratiques changeant souvent d'URL, de présentation, ou disparaissant régulièrement.

160. - « Jeux Internet. Attention aux pièges ! », article *letelegramme.com* du 3 janvier 2010.

161. - V. <http://www.habbo.fr/credits>.

162. - Article précité. La somme atteinte, au regard des plafonds précités associés au système « Internet plus » s'explique sans doute par le caractère professionnel de l'abonnement (le plafond est alors plus élevé, comme nous l'avons indiqué), associé à une absence de réaction immédiate à réception de la première facture anormale.

163. - On peut à présent y lire : « Internet Plus permet d'acheter avec ton abonnement à Internet. En l'utilisant, tu utilises des vrais euros, ce n'est pas gratuit ! Demande l'autorisation à tes parents avant de l'utiliser ! Ton achat apparaîtra sur ta facture Internet (ou celle de la personne qui paye ton abonnement Internet) ».

299. **Preuve du contrat** - Mais de quelle preuve disposerait le fournisseur de contenu, si l'existence du contrat était niée par son client ? Ici, aucun formulaire n'est rempli, aucune adresse de livraison n'est précisée, et, surtout, aucun moyen de paiement personnel à son porteur n'est employé. Il ne reste donc qu'une trace informatique de la transaction dans les logs d'un serveur. Toutefois, la valeur probante de ces *logs* pourrait être renforcée en l'espèce par le fait que c'est le FAI qui enregistre le paiement, et non le fournisseur de contenu. Au moment de payer, en effet, le client est redirigé vers une page appartenant non au vendeur de sonnerie de téléphone, de « crédit Habbo », etc., mais à son FAI. Ce prestataire apparaît du point de vue de la transaction comme un tiers — comme un tiers intéressé toutefois, par la perception d'une commission — ce qui pourrait le faire apparaître aux yeux du juge comme plus fiable. Il n'y aura donc, pour convaincre que le juge, que la seule présomption tirée de ce document. Toutefois, ce *log* pointe non pas vers un individu déterminé, mais vers une adresse IP. Éloignons-nous un instant de l'idée de fraude strictement familiale : l'IP aurait pu être usurpée par un pirate ; un simple ami de passage dans le foyer aurait pu se trouver aux commandes du poste informatique ; un voisin auquel on aurait accordé un droit temporaire d'user de l'accès Internet en wifi aurait pu en profiter pour faire des achats via « internet plus »¹⁶⁴. Dans son appréciation de la solidité de la présomption, le juge devrait tenir compte de ces possibilités. Revenons à notre hypothèse : ce pourrait ne pas être l'abonné lui-même, mais par exemple l'un de ses enfants, qui a contracté. Or, les concepts classiques du droit des obligations ne permettent pas d'imputer l'opération contractuelle au foyer sans plus de précision. Allons plus loin : s'il était possible de prouver que c'est l'enfant qui a passé l'opération¹⁶⁵, il serait théoriquement possible au parent d'agir contre le fournisseur de contenu en répétition de l'indu, car il a payé sans être débiteur ; à charge pour le fournisseur de contenu de se retourner ensuite contre l'enfant¹⁶⁶.

300. **Obligation occulte de surveillance de l'accès à Internet** - Nous constatons donc que de tels contrats peuvent être attaqués sous de multiples angles. Mais tout cela est destiné à rester pure spéculation théorique, tant il est certain que personne ne se donnera la peine d'agir en justice pour de pareils montants. Surtout, le véritable problème posé par ce type de système de paiement se situe à un autre niveau. Pourquoi ne pas admettre qu'il pèse sur le souscripteur de l'abonnement un véritable devoir de surveiller l'usage qui est fait de ses postes informatiques ? Les conditions

164. - Ce cas a été raconté sur un forum. Une personne avait accepté de « dépanner » un voisin qui venait d'emménager en lui donnant accès à son réseau wifi. Elle ignorait, comme beaucoup, que cela rendait possible une facturation sur sa tête de prestations payées via « Internet plus ».

165. - Cela semble presque impossible, encore qu'on puisse faire à nouveau appel à une présomption de fait, tirée par exemple du type de contenu acheté, lorsque ce contenu est clairement destiné aux enfants.

166. - Poursuivons cette pure hypothèse d'école : si l'enfant a un patrimoine, le parent pourrait à nouveau avoir à payer, mais ès qualités d'administrateur légal de ses biens.

générales sont d'ailleurs d'ores et déjà en ce sens : « [...] L'Abonné est notamment seul responsable de l'utilisation du service paiement Internet Orange [...] toute connexion ou transmission de données effectuées en utilisant le service Paiement Internet Orange seront réputées avoir été effectuées par l'Abonné (...) et s'effectue sous sa responsabilité exclusive »¹⁶⁷. De plus, les problèmes probatoires peuvent être écartés par une convention de preuve, dont l'efficacité est ici envisageable, puisque les conditions générales qui la contiennent font l'objet d'une classique signature autographe lors de la souscription en boutique¹⁶⁸. Cette combinaison de clauses aboutirait à ce que le titulaire de l'abonnement ait effectivement à supporter sur son patrimoine tous les paiements réalisés via son adresse IP. Mais est-ce acceptable ? À propos de l'affaire de la Maison des jeunes de Questembert, une animatrice s'exclame : « Personne ne savait que cela existait »¹⁶⁹. Ce sentiment est partagé sur de nombreux forums d'utilisateurs mécontents de ce système de paiement: personne n'était au courant qu'il était possible à ses enfants ou à un ami de passage de battre monnaie à partir de l'autorisation de prélèvement donnée au FAI à la souscription de l'abonnement¹⁷⁰. Du moins cette surprise se retrouvait-elle parmi les abonnés aux opérateurs acceptant d'activer le système par défaut, sans exiger aucune donnée d'authentification pour valider la première utilisation.

L'étude a montré que le processus de conclusion des contrats par voie électronique prenait la forme de procédures simples et rapides, au prix d'une double fragilité : celle du consentement, si peu éclairé et si peu dense qu'on en vient à douter qu'une authentique rencontre des volontés se soit produite, et celle des preuves que la convention a bien été passée, par une personne identifiée. Mais lorsque les technologies numériques sont mises au service de l'exécution du contrat, le laxisme peut faire place à la rigueur.

167. - Article 9 des « Conditions spécifiques relatives aux solutions de paiement Orange » (9 février 2017).

168. - Elles ne se heurtent donc pas à l'impossibilité logique que nous décrivions plus haut (supra, n° 290). Ainsi, l'art. 22 des « conditions générales de l'offre Livebox initiale » (6 avril 2017) stipule : « Pour les besoins du présent Contrat, les Parties conviennent que l'écrit sous forme électronique est admis comme support probant au même titre que l'écrit sur support papier. Les Parties conviennent de conserver les enregistrements informatiques et les copies papier des messages ou commandes qu'elles s'échangent pour l'exécution du présent Contrat de telle manière qu'ils puissent constituer des copies fidèles et durables au sens de l'article 1348 (sic) du code civil ». Ce texte pose cependant un problème puisqu'il ne fait que reprendre l'équation déjà posée par le Code civil selon laquelle l'écrit électronique équivaut à l'écrit papier ; or, les logs des serveurs Orange conservant la trace des transactions « Internet plus » ne sont pas, selon nous, des écrits électroniques.

169. - Article du Télégramme précité.

170. - De très nombreux internautes, dont l'auteur, ont découvert l'existence du système « Internet plus » en lisant la planche de Martin Vidberg, « Les paiements en ligne sont (presque) sécurisés », parue le 5 avril 2011 sur le blog de l'auteur, www.vidberg.blog.lemonde.fr.

II – L'idéal de rigueur dans l'exécution des contrats

301. **Plan** – Des automatismes numériques peuvent être placés au service d'une exécution rigoureuse des conventions. Il faudra les décrire (A), avant de souligner les risques dont ces évolutions sont porteuses (B).

A – Les moyens de l'exécution automatisée

302. **Concept de smart contract** – Nous avons présenté plus haut la *blockchain*, ce registre de transactions réputé infalsifiable, dont la mise en ordre est le fruit d'opérations décentralisées réalisées, sur les ordinateurs des internautes, par des armées de clercs algorithmiques¹⁷¹. Dans sa pureté originelle, il n'est pas davantage qu'un grand journal. Il est toutefois possible d'ajouter des couches logicielles en amont et en aval du processus de passation des écritures, afin de donner naissance à des fonctionnalités nouvelles. L'une des plus prometteuses est appelée *smart contract*¹⁷². L'appellation est trompeuse. Il ne s'agit pas ici de graver, au sein de la *blockchain*, le texte ou la photographie d'un contrat classique, rédigé dans un français courant ou juridique, afin d'apporter ultérieurement la preuve de son existence ou de son imputabilité. Non : le *smart contract* est composé à l'aide d'un langage de programmation. Il est interprété par une couche logicielle ajoutée à la *blockchain*. Y sont énumérées certaines conditions qui, si elles se réalisent à l'avenir, appelleront le déclenchement de certains effets.

L'un des exemples proposés en doctrine est le contrat de location saisonnière : le logiciel, constatant que le loyer n'a pas été viré sur le compte du bailleur avant une certaine date, enverrait à la serrure électronique équipant le logement l'ordre de se verrouiller¹⁷³.

Une plateforme nommée Ethereum a été spécifiquement inventée pour faciliter la mise en place de tels projets : sur la base d'une chaîne de blocs, elle propose d'échanger une cryptomonnaie appelée Ether, et offre une surcouche logicielle dédiée à la mise en place de *smart contracts*, basée

171. - V.supra, n°282.

172. - C. Zolynski, « Blockchain et smart contracts : premiers regards sur une technologie disruptive », *RDBF*, n° 1, janvier 2017, dossier 4 ; G. Guerlin, « Considérations sur les smart contracts », *Dalloz IP/IT*, octobre 2017 ; C. Bondard, et al., « Blockchain – Quelques utilisations actuelles de cet outil en droit des affaires. Monnaies virtuelles, transmission des instruments de paiement, outils de financement, smart contracts, etc. », *JCP E*, 2017, n° 36, 1471 ; E. Caprioli et al., « Blockchain et smart contracts : enjeux technologiques, juridiques et business », *Cahiers de droit de l'entreprise*, n° 2, mars 2017, entretien 2 ; T. Verbiest, « Quelle valeur juridique pour les smart contracts ? », *RLDA*, 2017, n° 129 ; A. Touati, « Tous les contrats ne peuvent pas être des smart contracts », *RLDC*, 2017, n° 147.

173. - A. Touati, « Tous les contrats... », art. préc.

sur un langage de programmation baptisé Solidity¹⁷⁴. Une grande compagnie d'assurance s'en est par exemple servie pour offrir une couverture automatisée du risque de retard en matière de transport aérien. La *blockchain* contrôle par elle-même les horaires d'arrivée des vols, et paie les indemnités en toute indépendance¹⁷⁵. Dans un tout autre domaine, un chercheur en sécurité a conçu une plateforme publique permettant à chacun de tester la solidité d'un mot de passe. L'organisateur du défi paie par avance une somme d'argent à titre de récompense, et fournit une empreinte chiffrée de son sésame (un *hash*), à partir de laquelle les participants pourront tenter de retrouver la clé en clair. Le réseau Ethereum est capable, de manière décentralisée, de vérifier la validité des mots de passe qui lui sont proposés et, en cas de succès, de payer automatiquement la récompense¹⁷⁶.

Une différence technique existe entre les deux exemples. Dans le cas de l'assurance contre le retard aérien, la blockchain est obligée de se connecter à des modules externes — dénommés « oracles » par la pratique — : pour savoir si le vol est arrivé à l'heure, elle dépend d'une base de données tenue par un tiers ; pour régler l'indemnité en euros, elle doit donner un ordre à un service de paiement. Ce sont autant de vulnérabilités susceptibles d'entacher le parfait fonctionnement d'ensemble. Dans le cas de la récompense octroyée pour la découverte d'un mot de passe, la blockchain vérifie par ses propres moyens la validité de la réponse qui lui est proposée, et verse une récompense dans sa propre crypto-devise, dont elle a l'entier contrôle.

303. Les smart contracts sont-ils des contrats ? - L'expression « *smart contract* » apparaît pour la première fois en 1996, sous la plume de l'informaticien Nick Szabo¹⁷⁷. Ces contrats sont définis comme suit :

*New institutions, and new ways to formalize the relationships that make up these institutions, are now made possible by the digital revolution. I call these new contracts "smart", because they are far more functional than their inanimate paper-based ancestors. No use of artificial intelligence is implied. A smart contract is a set of promises, specified in digital form, including protocols within which the parties perform on these promises*¹⁷⁸.

Le fait que les contrats « de papier » soient présentés comme les ancêtres des contrats « intelligents » est susceptible d'être mal interprété. On pourrait croire qu'il s'agit de remplacer un

174. - www.ethereum.org.

175. - L'exemple était proposé par C. Zolynski, « Blockchain et smart contracts... », art. préc. L'idée a en effet été mise en œuvre par une compagnie d'assurances : <http://fizzy.axa>.

176. - G. Pépin, « Sur Ethereum, une plateforme décentralisée de craquage de mots de passe », article *nextinpact.com* du 4 août 2017.

177. - N. Szabo, « Smart contracts : building blocks for digital markets », consultable par ex. sur http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart_contracts_2.html.

178. - *Ibid.*

objet juridique par un autre, plus abouti. En réalité, M. Szabo ne se soucie nullement de cantonner sa réflexion à l'intérieur des limites du droit. Si les concepts juridiques ne peuvent être entièrement écartés de son analyse, c'est parce qu'il serait long et coûteux de repenser l'organisation sociale à partir de rien : il faut donc selon lui *s'inspirer* du droit comme système de régulation pour bâtir un ordre normatif distinct, plus puissant et plus efficace¹⁷⁹. La place occupée par le droit dans l'arbre généalogique des *smart contracts* est relativisée davantage encore lorsque M. Szabo compte les distributeurs automatiques de chips ou de boissons parmi les ancêtres immédiats de son invention.

A canonical real-life example, which we might consider to be the primitive ancestor of smart contracts, is the humble vending machine. Within a limited amount of potential loss (the amount in the till should be less than the cost of breaching the mechanism), the machine takes in coins, and via a simple mechanism, which makes a beginner's level problem in design with finite automata, dispense change and product fairly. Smart contracts go beyond the vending machine in proposing to embed contracts in all sorts of property that is valuable and controlled by digital means. Smart contracts reference that property in a dynamic, proactively enforced form, and provide much better observation and verification where proactive measures must fall short.

Le cadenas était une métaphore récurrente des mesures techniques de protection utilisées dans le domaine du droit d'auteur¹⁸⁰. Le choix d'un distributeur automatique comme symbole du *smart contract* à l'ère pré-numérique est du même ordre. Il s'agit toujours de décrire une régulation — du droit de propriété, du droit des obligations — par l'objet et par la technique plutôt que par le droit. Nous voici renvoyés à l'introduction de cette étude qui, dans la lignée des démonstrations de M. Lessig, identifiait droit et numérique comme deux ordres normatifs distincts. Cette altérité est le prélude de relations, qui peuvent être d'ignorance mutuelle, de collaboration ou d'affrontement. Une machine à café est un serviteur loyal de la volonté contractuelle des parties, mais elle n'est pas un contrat. De même, le *smart contract* n'est pas un contrat au sens que le droit donne à ce mot¹⁸¹. Il est, au mieux, une sentinelle numérique placée au service d'un contrat¹⁸². Dans ce cas, le lien

179. - *Ibid.* : « Over many centuries of cultural evolution has emerged both the concept of contract and principles related to it, encoded into common law. Algorithmic information theory suggests that such evolved structures are often prohibitively costly to recompute. If we started from scratch, using reason and experience, it could take many centuries to redevelop sophisticated ideas like property rights that make the modern free market work »

180. - V. *supra*, n° 230.

181. - En ce sens notamment : C. Zolynski, « Blockchain et smart contracts... », art. préc. ; G. Guerlin, « Considérations sur les smart contracts », art. préc.

182. - P. de Filippi, « Il faut davantage enseigner la technologie aux juristes », entretien avec le cabinet Deloitte sur *equationdelaconfiance.fr*, non daté : « (...) un smart contract est simplement un logiciel, une application de la blockchain. Comme on leur a donné l'appellation de "smart contracts", on a tendance à les assimiler à des contrats, alors qu'ils n'ont pas en eux-mêmes d'autorité juridique. Bien sûr, un logiciel peut implémenter un contrat. Dans ce cas, on revient au système des DRM (Digital rights management) qui intègrent à la fois un contrat de droit d'auteur et une technologie qui implémente ce contrat par le code. Lorsqu'un contrat juridique existe, le smart contract n'est qu'une application technique de ce contrat ».

fonctionnel qui existe entre eux pourrait être exploité, au besoin, sur le terrain probatoire. De même que l'introduction d'une pièce et la pression sur un bouton d'un distributeur d'en-cas rend vraisemblable l'existence d'un contrat sous-jacent entre l'exploitant de la machine et le client, la mise en place d'un commun accord d'un morceau de code informatique pourrait constituer l'ombre portée d'un contrat. Pourquoi l'assureur Axa aurait-il programmé dans une blockchain que le retard de plus de 30 minutes de l'avion de M. Dupont devait entraîner le versement de 70 euros en sa faveur, si ce n'était en raison de la conclusion préalable d'un contrat d'assurance couvrant ce risque ? Encore faudra-t-il que tout moyen de preuve soit admis s'agissant du contrat considéré.

La nature des *smart contracts* ayant été éclaircie, il reste à déterminer de quels effets pour le système juridique leur généralisation serait porteuse.

B – Les risques de l'exécution automatisée

304. **Motifs de recours aux smart contracts** – Dans certaines situations, il est facile de voir l'arrivée d'un automatisme numérique d'exécution comme un progrès. Le *smart contract* se présente comme un tiers de confiance immatériel et incorruptible chargé d'assurer la bonne fin des obligations contractuelles. Reprenons l'exemple de l'assurance contre les retards dans le transport aérien : la vidéo de présentation souligne qu'il n'y a « pas de déclaration de sinistre, pas de formulaire, pas de temps perdu »¹⁸³. Les sommes en jeu sont faibles. Dès lors, l'assuré ne veut pas perdre son temps à déclarer la réalisation du risque ni son énergie à batailler contre l'éventuelle inertie de son partenaire contractuel. Quant à l'assureur, s'il devait confier de si petits dossiers à ses services de règlement des sinistres, cela engendrerait des coûts qui feraient chuter sa compétitivité, allant peut-être jusqu'à oblitérer la possibilité de proposer semblable couverture. À plus forte raison, il n'est pas envisageable d'impliquer des tiers de confiance humains tels qu'un expert ou un juge dans des dossiers aussi simples que modiques.

Dans le cas de contrats d'une valeur économique plus importante, la rémunération d'un tiers de confiance humain n'est plus une difficulté rédhibitoire. Dès lors, l'existence d'un soutien numérique à l'exécution ne constituera pas une condition de leur existence même, mais un simple facteur de diminution des coûts ou d'intensification de la confiance. Les conventions les plus propres à être doublées d'un *smart contract* sont celles qui présentent, avant même le recours à l'informatique, le plus haut degré d'automaticité et d'élémentaire brutalité dans leur exécution. Les deux exemples les plus évidents sont alors le crédit documentaire et sa cousine, la garantie autonome à première demande. Dans le premier cas, une banque est chargée de verser une somme d'argent, représentant

183. - fizzy.axa.

un paiement, aussitôt que lui est présenté un document attestant que la prestation ainsi réglée a bien été effectuée. Ainsi, dans le commerce maritime, plutôt que d'en passer par une banque à qui l'on enverra par fax ou email un document attestant d'une livraison par un navire, on pourrait équiper les conteneurs transportés de puces GPS, et déclencher le règlement par une *blockchain* dès que les coordonnées spatiales du port de destination sont atteintes¹⁸⁴. Dans le second cas, celui de la garantie autonome, le bénéficiaire de la sûreté personnelle a accepté de renoncer à ce qu'un gage-espèces, plus protecteur, soit constitué *ab initio* entre ses mains. Mais c'est à la condition qu'il puisse, d'un simple courrier, obliger une banque à lui virer la même somme, pour le cas où l'exécution du contrat de base lui semblerait mal se dérouler¹⁸⁵. Une confiance égale ou même supérieure pourrait théoriquement être suscitée par un *smart contract* dans lequel un clic de souris remplacerait l'envoi du courrier.

Mais les avantages ainsi recensés ne doivent pas occulter les inconvénients éventuels du recours aux *smart contracts*.

305. Dangers du recours aux smart contracts – La plateforme Ethereum a connu récemment un incident de fonctionnement à 50 millions de dollars. Un groupe d'utilisateurs y faisait fonctionner une plateforme appelée *the Decentralized Autonomous Organization* (the DAO), dont les principes étaient fort ingénieux. Il s'agissait d'un fonds d'investissement dans lequel les décisions étaient prises collectivement : les membres votaient pour déterminer dans quelles sociétés placer leurs fonds. Hélas, un utilisateur parvint à faire conclure au fonds un *smart contract* contenant une « erreur » de code, dont on peut soupçonner qu'elle était volontaire, et qui faisait tourner en boucle un ordre de paiement au lieu de le déclencher une seule fois¹⁸⁶. L'argent mal acquis n'a pas pu être dépensé : en vertu des principes des *blockchains* publiques, chaque Ether ainsi obtenu pouvait être suivi individuellement, de sorte que sa dépense pouvait être empêchée. Par

184. - En ce sens : D. Legeais, « L'apport de la blockchain au secteur bancaire », communication lors du colloque L'apport des fintechs au droit bancaire, colloque du 17 novembre 2016, CEDAG, sous la co-responsabilité du sus-cité et de Mme Nathalie Martial-Braz.

185. - Il existe plusieurs variétés de garanties autonomes. La plus rigoureuse est stipulée « à première demande pure et simple » et s'accorde très facilement avec le concept de smart contract. Mais même la variété « à première demande justifiée » requiert simplement que l'appel soit motivé, sans que la banque n'aie le droit d'étudier le bien-fondé des arguments présentés (qui seront seulement conservés pour être employés dans l'éventuel contentieux ou arbitrage qui suivra). Il n'y a donc pas d'obstacle à ce qu'un smart contract soit employé, qui ouvre une boîte de dialogue avant de déclencher le paiement. En revanche, la garantie autonome documentaire, de même que le crédit documentaire, oblige à recourir à un « oracle » pour que la blockchain ait accès à des informations sur le monde extérieur.

186. - K. Finley, « A \$50 million hack just showed that the DAO was all too human », article *wired.com* du 18 juin 2016 ; K. Hottot, « The DAO : un pirate dérobe 50 millions de dollars, la contre-attaque se prépare », article *nextinpact.com* du 22 juin 2016. Les articles spéculent sur la nature exacte de l'erreur de code, qui n'est pas connue dans ses détails.

la suite, une réécriture de la blockchain Ethereum a été décidée par un vote majoritaire de ses utilisateurs afin « d’effacer » ce détournement¹⁸⁷.

Même si les dégâts consécutifs à cet incident ont été minimisés, l’histoire est riche d’enseignements. Elle rappelle d’abord que tout objet informatique est susceptible d’attaques. La prise de contrôle hostile d’une blockchain publique n’est pas impossible. Les « oracles » sont également susceptibles d’être visés : imaginons que la base de données des retards aériens sur laquelle se base Axa fasse l’objet d’une attaque informatique destinée à faire apparaître tous les vols comme défaillants : l’ensemble des contrats donneraient lieu au versement immédiat d’une indemnité. Et puis, l’affaire the DAO le montre, une « clause » informatique du *smart contract* peut se révéler défectueuse, par accident ou par malice.

Mais au-delà des problèmes de sécurité informatique, cette affaire montre ensuite que le principal attrait du *smart contract*, son automaticité totale, constitue parfois sa plus grande faiblesse. Rappelons ici les propos du rapporteur de la loi « informatique et libertés », qui soulignait « l’absence de faculté d’étonnement » des ordinateurs et mettait en garde contre toute prise de décision algorithmique qui ne serait pas supervisée par l’humain. C’est la même cécité dont on prône tantôt l’efficacité et dont on redoute tantôt l’injustice.

Nous avons vu que le *smart contract* n’était pas un contrat : il en est au mieux le décalque logiciel, pensé exclusivement à des fins de rigoureuse exécution. Il en résulte un objet aveugle aux vices de conception, comme dans l’affaire the DAO, mais aussi incapable d’appliquer des concepts mous comme la bonne foi, le raisonnable ou le manifestement excessif. Les conditions de son fonctionnement ne peuvent être trop subtiles : un produit d’assurance classique, avec sa batterie d’exclusions conventionnelles de risques et de conditions de garantie, devrait être branché sur une multitude d’oracles, et avoir la capacité d’interpréter leurs informations. En introduction de cette étude, discutant du concept de justice prédictive, nous disions nos doutes sur la capacité du raisonnement juridique à être réduit à une succession de pures opérations de logiques formelles¹⁸⁸. La superposition du contrat de droit et de son bras armé numérique sera par conséquent toujours grossière. Ce qui sera implacablement exécuté, c’est une esquisse, et parfois une caricature de contrat. Le constat est d’autant plus fort pour les conventions complexes, mais il n’épargne pas les accords les plus simples. Un contrat élémentaire a pu être conclu par violence ou par dol, ou contenir une clause abusive : le programme restera sourd à ces arguments, et procédera à l’implacable exécution.

187. - K. Hottot, « Ethereum : un “hard fork” controversé pour oublier the DAO », article *nextinpact.com* du 20 juillet 2016.

188. - V.supra, n°17.

Ainsi, la transformation de la norme juridique en une norme numérique l'expose à un net appauvrissement. Or, il est à craindre que ce processus ne présente pas les mêmes dangers pour les deux parties. Après avoir présenté un contrat de location d'automobile qui rend le véhicule impossible à démarrer si le loyer n'est pas payé, un auteur écrit :

(...) il n'est pas inintéressant d'analyser la manière dont les smart contracts sont concrètement exploités. On a vu que ces programmes pouvaient servir à prononcer des sanctions automatiques, notamment en bloquant un véhicule. Il est préoccupant de constater que, pour l'heure, ces sanctions semblent unilatérales : elles sont essentiellement conçues et programmées en faveur d'une partie forte, à l'encontre des parties acceptantes. Le plus souvent, c'est ainsi une banque créancière ou une société de location qui bénéficient de l'usage du smart contract, par la sanction infligée au débiteur défaillant. L'inverse n'est que rarement vrai : en cas de défaillance de la partie forte, les smart contracts ne semblent généralement pas programmés pour sanctionner leurs concepteurs. L'intelligence du smart contract est surtout celle de son programmeur¹⁸⁹.

Le constat rejoint celui que nous avons dressé en matière de mesures techniques de protection : entre les mains d'acteurs puissants, ces outils présentent d'importants dangers. Aux excès des contrats d'adhésion, qu'au moins le système juridique a appris à connaître et à tempérer, pourraient s'ajouter bientôt les *smart contracts* d'adhésion. Ils ne dépossèderaient pas la partie faible de sa capacité à invoquer le système juridique, mais elle ne pourrait le faire que dans un second temps. Selon une logique bien connue en matière de garanties autonomes, il faudrait payer d'abord — ou être mis à la porte de son logement, ou de son véhicule — et discuter ensuite¹⁹⁰.

Nous avons relevé que la multiplication annoncée des objets connectés favoriserait la multiplication de mesures techniques de protection potentiellement injustes : elle pourrait aussi encourager l'essor de *smart contracts* déséquilibrés, qui doubleraient les contrats classiques comme une seconde peau. Après le droit des biens, c'est donc le droit des obligations qui est menacé par la concurrence puissante de la normativité numérique.

À présent qu'ont été décrits les bouleversements entraînés par les technologies de l'information dans le droit commun des contrats, il faut aborder les évolutions qu'elles ont suscitées dans les droits spéciaux.

189. - G. Guerlin, « Considérations sur les smart contracts », art. préc.

190. - Lorsque le logement constitue la résidence principale du locataire, une telle expulsion de fait serait évidemment illégale. Cela explique que l'exemple souvent repris de la fermeture d'une serrure connectée par un smart contract soit systématiquement associé à une hypothèse de location d'agrément.

Section 2 – Droits spéciaux des contrats

306. **Communautés et nouveaux modes de production** – Dans la partie de cette étude consacrée à la communication, nous avons relaté la perte d'influence du modèle pyramidal de diffusion de l'information – un petit nombre de producteurs de contenus s'adressait auparavant à la multitude. Les messages sont aujourd'hui largement échangés de pair-à-pair : des individus placés sur le même plan sont à la fois producteurs et consommateurs de discours¹⁹¹. Cet apparent chaos pourrait être ordonné autour de centres d'intérêt, en cercles concentriques. Plutôt qu'une immense, abstraite et utopique communauté mondiale, pourraient être identifiés des milliers de groupes de tailles très variables, structurés autour d'une curiosité, d'un goût ou d'une passion qu'ils ont en partage. Comme l'a écrit Madame Clément-Fontaine, l'ère numérique est peut-être celle du retour en grâce d'un concept tombé en désuétude : celui de communauté¹⁹². Chacun, si atypiques soient ses goûts, si pointues soient ses connaissances, si marginales soient ses aspirations, fait partie d'une grande famille à l'échelle du monde.

Des simples échanges et discussions à la production collective d'objets intellectuels, tels que des encyclopédies ou des logiciels, il n'y a qu'un pas. Ainsi, « [...] le réseau Internet va devenir le siège des communautés, en particulier des communautés épistémiques. Une communauté épistémique peut se définir comme la réunion de personnes autour d'un projet qui forment de la sorte un groupe, non doté de la personnalité juridique, mué par une communauté d'intérêts, visant à produire et partager des connaissances encyclopédiques ou techniques (...) »¹⁹³. Les contributeurs de l'encyclopédie Wikipédia peuvent légitimement être saisis d'une fierté mêlée de vertige en contemplant l'incroyable résultat auquel ils sont parvenus, phrase après phrase, à force d'empiler des parcelles de connaissance. La démonstration est faite que les petits ruisseaux forment les grandes rivières. Mais cela se vérifie encore si l'on bascule des biens non rivaux que sont les richesses informationnelles vers le monde des biens rivaux. Qu'une personne ait un repas à

191. - V.supra, n°123.

192. - M. Clément-Fontaine, « La genèse de l'économie collaborative : le concept de communauté », *Dalloz IP/IT*, 2017, 140. L'auteur rappelle comment les corps intermédiaires avaient soumis leurs membres à une tutelle oppressante. Soucieuse d'émancipation, la Révolution française les disloque, mais laisse l'individu seul face à l'État. L'apparition ultérieure des sociétés ne comble pas ce vide : pour une petite fraction de la population, elles sont un outil de concentration des moyens de production, mais elles ne constituent pas un débouché général pour des citoyens en quête de sens, qui rechercheraient l'appartenance à un tout qui les dépasse. Les associations servent davantage un tel projet, mais l'auteur estime que « La loi du 1er juillet 1901, qui reconnaît la liberté d'association, ne fait pas disparaître toute trace de défiance à l'égard de ces organisations. Les règles qui encadrent le système associatif visent à préserver les libertés individuelles afin qu'elles ne pâtissent pas de l'organisation collective ».

193. - *Ibid.*

partager, une place dans sa voiture, une chambre inoccupée est une information anodine. Mais des milliers, des millions de propositions de ce type à travers le monde, une fois agrégées par les forces de traitement numériques, constituent des réservoirs de richesse d'une profondeur inouïe.

307. L'introuvable économie collaborative - De telles méthodes peuvent être placées au service des fins les plus désintéressées comme du capitalisme le plus débridé. En faire tomber l'ensemble des usages sous un seul et même concept, c'est la certitude de forger une notion décevante. C'est toute l'histoire de l'expression « économie collaborative »¹⁹⁴. En anglais, c'est plutôt la formule *sharing economy* (économie du partage) qui se rencontre le plus fréquemment¹⁹⁵.

Certains projets sont indiscutablement placés sous le signe de la générosité désintéressée. Dans le domaine des biens de la connaissance, plusieurs exemples ont déjà été proposés. En matière de biens rivaux, la plateforme *Couchsurfing* propose d'accueillir chez soi, bénévolement, des voyageurs de passage. La seule contrepartie mise en avant est une expérience humaine, et la possibilité d'être à son tour accueilli chez un autre membre du réseau : le concept de « communauté » conserve ici tout son sens. L'intermédiaire lui-même n'est pas rémunéré.

À l'autre bout du spectre des valeurs, une société comme Uber propose à ses utilisateurs un service de transport urbain géolocalisé bien connu. Les chauffeurs sont rémunérés, et tirent souvent de cette activité l'essentiel de leurs revenus. La plateforme prélève une forte commission. Il n'y a pas la moindre trace de « partage » dans un tel modèle d'affaires. Aucune communauté ne peut être identifiée : il n'y a qu'une clientèle. Pour des entreprises de ce type, promouvoir un concept « d'économie collaborative » qui fasse d'elles les voisins de palier de Wikipédia est une excellente opportunité sur le plan de l'image : c'est ce que certains auteurs appellent le « *sharewashing* »¹⁹⁶.

Entre ces deux extrêmes existe une gigantesque zone grise. Le critère de l'économie collaborative se trouve-t-il dans la gratuité des services ? Dans ce cas, une plateforme d'échange de recettes comme Marmiton, voire un réseau social comme Facebook doivent en relever, quand bien

194. - Sur laquelle V. not., outre l'article précité de M. Clément-Fontaine, « La genèse de l'économie collaborative... » : S. Moreil, « Economie collaborative : alternative au capitalisme ou ubérisation de l'économie ? », *Cahiers de droit de l'entreprise*, mai 2017, n° 3, dossier 10, ainsi que l'ensemble des actes de colloque que cet article introduits, et spéc. S. Chassagnard-Pinet, « À la recherche d'une définition de "l'économie collaborative" », article 11 ; A. Lecourt, « Quelles pistes juridiques pour encadrer l'économie collaborative ? », *RLDA*, N° 117, juillet 2016 ; P. Terrasse (dir.), *Rapport au Premier ministre sur l'économie collaborative*, février 2016 ; Commission européenne, *Un agenda européen pour l'économie collaborative*, COM.(2015) 356, 2 juin 2016 ; Parlement européen, *Résolution sur un agenda européen pour l'économie collaborative*, 2017/2003(INI), 15 juin 2017.

195. - Pour une tentative de définition de l'expression « économie du partage » comme distincte d'« économie collaborative » : S. Chassagnard-Pinet, « À la recherche... », art. préc.

196. - S. Chassagnard-Pinet, « A la recherche... », art. préc., citant A. Kalamar, « Sharewashing is the New Greenwashing », article *opednews.com*, 2013.

même les opérateurs se rémunèrent grâce à de la publicité ciblée ou à l'exploitation de données personnelles. Faut-il alors rechercher des services fonctionnant sans but lucratif ? La plateforme « La machine du voisin » permet à celui qui n'aurait pas de quoi laver son linge d'entrer en contact avec une personne équipée. Le site lui-même ne perçoit aucune commission et a été créé dans un esprit de pur désintéressement. En revanche, les utilisateurs fixent d'un commun accord la somme qui sera versée au propriétaire de la machine, qui est au moins un défraiement, mais peut aller jusqu'à constituer un bénéfice. Autre exemple difficile à saisir, la plateforme Helloasso propose des instruments de financement participatif au monde associatif. Elle propose au donateur de lui réserver, à titre facultatif, une part de sa libéralité. Ses services sont donc potentiellement gratuits, ce qui peut très bien constituer un habile modèle d'affaires. Sont-ce les objectifs poursuivis par les utilisateurs qui doivent retenir l'attention ? Envisageons alors le cas de Blablacar : la plateforme de covoiturage gagne de l'argent, mais les motivations des usagers sont quant à elles très diverses. Certains participent pour des raisons avant tout financières, d'autres par souci de préservation de l'environnement, d'autres encore pour faire des rencontres¹⁹⁷. De très nombreux projets supportent ainsi des lectures multiples : louer sa maison lorsqu'on en est absent quelques jours, sa voiture lorsqu'on ne l'utilise pas, la perceuse qui prend la poussière dans un placard, tout cela peut constituer le moyen de soulager la planète, en procurant une utilité maximale à des biens fabriqués à partir de ressources limitées. Ce peut être aussi l'amorce d'une monétisation des services d'amis, autrefois gratuits, permettant à l'argent d'asseoir son emprise sur les rares relations humaines qui lui échappaient encore¹⁹⁸.

Osant une définition, Mme Botsman voit dans l'économie collaborative « *An economy built on distributed networks of connected individuals and communities versus centralized institutions, transforming how we can produce, consume, finance, and learn* »¹⁹⁹. Le rapport sur l'économie collaborative rédigé par M. Terrasse à la demande du Premier ministre part s'approprier cette définition, qu'il fait immédiatement suivre d'une série d'exemples qui sont tous porteurs de progrès environnementaux ou humains substantiels²⁰⁰. Mais pour éviter que la définition soit si inclusive

197. - « Transport : le covoiturage ? Economique, sympathique et plus écologique ! », article *leparisien.fr* du 11 mai 2015.

198. - En ce sens : N. Mathey, « L'uberisation et le droit des contrats », communication lors du colloque *Le droit civil à l'ère numérique* du 21 avril 2017, Université Panthéon-Assas.

199. - R. Botsman, « The sharing economy lacks a shared definition », article *fastcompany.com* du 21 novembre 2013. Comp. la définition tautologique et molle proposée par la Commission européenne, *Un agenda européen...*, rapport préc., p. 3 : « Aux fins de la présente communication, le terme "économie collaborative" désigne des modèles économiques où des plateformes collaboratives qui créent un marché ouvert pour l'utilisation temporaire de biens et de services souvent produits ou fournis par des personnes privées facilitent des activités ».

200. - P. Terrasse (dir.), rapport préc., partie 1.1.2, intitulée « L'économie collaborative renvoie à des modes alternatifs de consommation et de production, dont seule une minorité passe par Internet ».

que même l'exemple-repoussoir Uber puisse s'y loger, il faut en réalité interpréter l'expression « transformant les modes de production, de consommation... » comme signifiant implicitement « transformant de manière vertueuse ». C'est une perspective politique plutôt que technique qui est ainsi proposée, tant les mérites des plateformes citées se discutent. À eux seuls, ils ne semblent pas constituer des critères suffisamment solides pour servir de points d'appui à des réglementations différenciées.

308. **L'économie de plateforme** - Accepter de se départir d'une approche moralisante de ces nouveaux services — au moins temporairement — laisse apparaître certaines structures d'organisation typiques qui, elles, posent indiscutablement des problèmes juridiques. Leur caractéristique commune consiste dans le recours à un site conçu pour organiser le face-à-face d'une offre et d'une demande : la plateforme.

S'agissant des réseaux sociaux, les utilisateurs offrent et recherchent des contenus, des publications. Ces services ouvrent leurs colonnes virtuelles à l'expression d'autrui sans assurer *a priori* aucun travail de sélection, de rédaction en chef, de mise en contexte comme pouvaient le faire les médias antérieurs. Ces difficultés particulières ont déjà été examinées dans la partie de l'étude dédiée aux communications électroniques²⁰¹. Par ailleurs, ceux de ces réseaux qui ont une vocation lucrative adoptent généralement un modèle économique fondé sur une « fausse gratuité », reposant sur la publicité ciblée et l'exploitation de données personnelles, autant de questions qui ont elles aussi déjà été abordées²⁰².

Quant aux plateformes visant à la création en commun de ressources intellectuelles utiles à tous, comme les encyclopédies ou les logiciels libres, leur principale préoccupation sur le plan du droit consiste à mettre en œuvre les règles relatives à la propriété intellectuelle d'une manière qui assure la circulation et la pérennité de l'œuvre commune²⁰³.

Subsiste alors la grande masse des plateformes assurant la répartition de ressources rivales, biens ou services. Leur rôle est d'assurer la rencontre entre une offre et une demande portant sur une place dans un moyen de transport, une chambre pour la nuit, une heure de bricolage ou de cours d'anglais. Auparavant, deux moyens s'offraient à celui qui recherchait ces prestations. Il pouvait avoir recours à son cercle amical ou familial, généralement à titre gratuit, essentiellement en marge du droit et de l'économie. Ou bien il pouvait s'adresser à un professionnel, ce dernier étant contraint d'atteindre une certaine taille critique ou de déployer des moyens suffisants pour assurer sa

201. - V.supra, n°155.

202. - V.supra, n° 57 s.

203. - V.supra, n°240.

notoriété. Une troisième solution s'offre désormais à lui : recourir à un intermédiaire en ligne pour trouver son futur partenaire contractuel.

309. **Le courtage 2.0** – Les professionnels de l'entremise existent depuis longtemps. Mais il s'agissait auparavant d'un travail confié à des compétences humaines, par conséquent lent et coûteux, qui ne devait être mobilisé que pour des opérations d'ampleur. Celui qui recherche un covoiturage à 15 euros ne peut évidemment doubler cette somme pour rémunérer un intermédiaire humain ni attendre plusieurs heures avant que son dossier ne soit ouvert alors qu'il souhaite voyager l'après-midi même. Un courtier algorithmique offre une réponse dans la seconde et réclame une commission bien inférieure. S'ouvrent alors aux intermédiaires le marché des micro-professionnels et celui du dilettantisme²⁰⁴. Un agglomérat suffisant de particules élémentaires fait naître des montagnes. Des secteurs entiers qui fonctionnaient sur le principe du tête-à-tête, généralement entre un client et un professionnel, s'ouvrent alors aux relations triangulaires. De plus, au sein du trio, la position de force n'est plus systématiquement détenue par celui qui va livrer le bien ou rendre le service : elle appartient plutôt à celui qui organise la rencontre. L'information, plus que jamais, est le véritable pouvoir. Quant à celui qui recherchait la chose ou la prestation, il voit lui aussi sa situation modifiée. S'il traite avec un professionnel de très petite surface, et plus encore avec un amateur, peut-il espérer recevoir les mêmes conseils, et bénéficier des mêmes garanties pour le cas où les choses tourneraient mal ? S'il est déçu, pourra-t-il orienter ses recours vers l'acteur le plus solide : celui qui s'est chargé de l'orienter ?

Analyser ces différentes évolutions impose de se tourner à la fois vers les contrats d'intermédiaire (I) et vers les contrats intermédiés (II).

I – Les contrats d'intermédiaire

310. **Plan** – Pour décrire le rôle des plateformes, le rapport Terrasse propose le terme de « prescripteur »²⁰⁵. Ces acteurs considèrent ne pas participer à l'échange économique sous-jacent : ils se trouveraient hors du marché, dans une position de surplomb. Par conséquent, ils seraient dispensés de se plier aux réglementations sectorielles parfois très lourdes applicables aux acteurs traditionnels (A). Il ne resterait qu'à leur appliquer le droit des contrats d'entremise, en particulier du courtage, éventuellement adapté à la marge à l'univers numérique (B).

204. - On désigne comme « dilettante » le cuisinier, le chauffeur ou le bricoleur d'un jour, qui facture son service tout en affirmant ne pas en tirer de revenu substantiel, mais simplement un défraiement ou de l'argent de poche.

205. - P. Terrasse (dir.), rapport préc., point 2.2.2.

A – Les plateformes en dehors du marché : une fonction d’entremise

311. **Plan** - Dans sa récente résolution relative à l’économie collaborative, le Parlement européen « invite la Commission à clarifier davantage, dans les plus brefs délais, les régimes de responsabilité des plateformes collaboratives, afin de promouvoir un comportement responsable, la transparence et la sécurité juridique, et d’accroître ainsi la confiance des utilisateurs ; observe, en particulier, l’incertitude concernant, en particulier, la question de savoir si une plateforme est fournisseur d’un service sous-jacent ou ne fait que proposer un service de la société de l’information [...] »²⁰⁶. Or, la réponse de principe est déjà connue : une véritable plateforme, qui renseigne sur le marché sans y prendre part, qui ne l’oriente pas directement, qui n’en altère pas le fonctionnement par sa présence, n’est pas soumise à la réglementation conçue pour un acteur de terrain (1). Mais ce principe trouve sa limite dès lors que la plateforme quitte sa posture de neutralité pour prendre la direction du marché qu’elle prétend surplomber (2).

1. – Le principe : l’entremise au profit du marché

312. **L’exemple du financement participatif** – Les plateformes de financement participatif constituent un exemple particulièrement frappant du phénomène d’ensemble qu’il s’agit ici d’illustrer, pour deux raisons²⁰⁷. La première, c’est qu’il s’agit d’un des rares secteurs dans lesquels le droit français a déjà été entièrement repensé pour tenir compte des nouveaux intermédiaires numériques : par conséquent, les règles qui seront présentées ne consistent pas en autant d’adaptations spéculatives du droit commun à un support nouveau, mais sont les éléments d’un statut complet décidé par les pouvoirs publics en toute connaissance de cause. La deuxième, c’est que les secteurs concernés — la banque et la finance — comptent parmi ceux qui font peser sur les acteurs de marché classiques les sujétions les plus draconiennes, les statuts les plus rigides : le fait que les plateformes en soient dispensées en tout ou partie n’en est que plus spectaculaire.

Le principe du financement participatif consiste à collecter de petites sommes auprès d’un large public²⁰⁸. Il est mis en œuvre par le Téléthon depuis les années 80, mais il n’y a de place, dans les

206. - Résolution précitée du 15 juin 2017, considérant 25.

207. - Nous tirons ici profit de certains des résultats de recherche présentés dans « Le financement participatif » in *Mélanges en l’honneur du professeur Didier R. Martin*, LGDJ, 2015, p. 479.

208. - Autorité des marchés financiers (AMF) et Autorité de contrôle prudentiel et de résolution (ACPR), *Guide du financement participatif à destination des plateformes et porteurs de projets*, 14 mai 2013, p. 1 : « Le crowdfunding (...) est un nouveau mode de financement de projets par le public. Ce mécanisme permet de récolter des fonds — généralement de petits montants — auprès d’un large public en vue de financer un projet artistique (musique, édition, film, etc.) ou entrepreneurial (...). Les opérations de crowdfunding peuvent être des soutiens d’initiatives de proximité ou des projets défendant certaines valeurs. Elles diffèrent des méthodes de financement traditionnelles et intègrent souvent une forte dimension affective

médias traditionnels à diffusion pyramidale, que pour quelques très grands projets. Internet donne sa place à tous, y compris aux plus petits. Le numérique leur offre une place illimitée pour se décrire, des outils multimédias pour convaincre, des moteurs de recherche et des classements par catégories pour être repérés. Sous une même appellation de *crowdfunding*, trois types de financements assez différents cohabitent en réalité : ceux par dons (le mécénat participatif), ceux par prêt (le prêt participatif) et ceux par prise de participation dans le capital d'une société (investissement participatif)²⁰⁹. Les porteurs de projets sont tantôt des artistes, qui demandent au public de financer une œuvre — un album de musique, un livre, un film, une bande dessinée — en contournant les bailleurs de fonds habituels du secteur que sont les éditeurs et les producteurs, tantôt des entrepreneurs, qui cherchent à emprunter ou à placer des parts de capital en suscitant directement l'enthousiasme des particuliers plutôt qu'en négociant avec des banques ou en s'aventurant sur les marchés financiers²¹⁰.

Si le droit français réserve aujourd'hui un accueil assez chaleureux à ces techniques, il n'en a pas toujours été ainsi : le premier réflexe des autorités de tutelle de la banque et de la finance a consisté à traiter les plateformes de financement participatif comme des acteurs de marché classiques.

313. La résistance initiale au modèle d'entremise – En mai 2013, l'AMF et l'ACPR ont publié conjointement un « Guide du financement participatif (crowdfunding) à destination des plateformes et des porteurs de projet »²¹¹. L'intitulé était trompeur : il s'agissait en réalité d'une longue démonstration de l'illégalité manifeste des plateformes de financement participatif aux yeux des régulateurs.

Lorsqu'il s'agissait d'organiser des campagnes portant sur de simples dons, on aurait pu croire que l'activité des plateformes n'empiétait guère sur les prérogatives du monde bancaire. L'ACPR contestait cette analyse. Puisque les plateformes recueillent des ordres de paiement et exécutent des ordres de virement, elles fournissent des services financiers au sens du Code monétaire et financier²¹². Par conséquent, les plateformes auraient dû être agréées comme établissements de

209. - V. par ex. P. Storrer, « Crowdfunding, bitcoin : quelle régulation ? », *D.*, 2014, p. 832.

210. - Cela n'exclut pas de compléter par la suite le tour de table en s'adressant à des bailleurs de fonds traditionnels. Comme l'écrit la Commission européenne, le financement participatif aide des start-up à progresser sur « l'escalier du financement » : une fois la confiance d'un large public de particuliers acquise, un établissement de crédit ou un capital-risqueur sera plus enclin à rejoindre le projet (Commission européenne, Communication du 27 mars 2014 au Parlement européen, au Conseil, au Comité économique et social européen et au Comité des régions, *Libérer le potentiel du financement participatif dans l'Union européenne*, p. 2 s.).

211. - Autorité des marchés financiers (AMF) et Autorité de contrôle prudentiel et de résolution (ACPR), *Guide du financement participatif*, précité.

212. - Art. L. 314-1, II, 3°, c et II, 5°. V. le *Guide* précité, p. 2.

paiement ou, *a minima*, agir en partenariat avec un prestataire de services de paiement agréé²¹³. À défaut, une peine de trois ans d'emprisonnement et 375 000 euros d'amende était encourue²¹⁴. À plus forte raison, lorsqu'il s'agissait de financement participatif sous forme de prêts, des frictions se produisaient avec la réglementation bancaire traditionnelle. Le raisonnement de l'ACPR était le suivant : dès lors que le prêt était rémunéré, il constituait une opération de crédit²¹⁵. Pratiquer de telles opérations de crédit à titre de profession habituelle nécessitait un agrément d'établissement de crédit²¹⁶. Ici encore, à défaut, de lourdes sanctions pénales étaient encourues²¹⁷. En exagérant à peine, on en conclura que pour exploiter légalement une telle plateforme, il aurait fallu être... une banque²¹⁸.

Le *Guide* se poursuivait sur le même mode par une litanie de reproches situés, cette fois-ci, sur le terrain du droit des marchés financiers. Les plateformes d'investissement participatif réalisaient plusieurs actes susceptibles d'être qualifiés de services d'investissement au sens du Code monétaire et financier : la « réception et transmission d'ordres pour le compte de tiers », mais aussi la formulation de « recommandations personnalisées (...) concernant une ou plusieurs transactions portant sur des instruments financiers »²¹⁹. L'AMF en déduisait qu'il était nécessaire pour la plateforme de demander un agrément de prestataire de service d'investissement ou de conseiller en investissements financiers²²⁰.

Ces réactions des autorités de tutelle étaient logiques, et l'on ne saurait leur en faire reproche. Les professionnels du crédit et des marchés financiers sont soumis à une lourde réglementation : ils doivent justifier de leur honorabilité, de leur compétence, de leur solvabilité, respecter de strictes règles prudentielles. Le monopole dont ils jouissent dans l'exercice de leur activité n'est pas édicté à titre principal dans leur intérêt : il profite avant tout au public. C'est la garantie, pour les clients,

213. - Art. L. 522-6 CMF.

214. - Art. L. 572-5 CMF.

215. - Art. L. 313-1 CMF al. 1 : « Constitue une opération de crédit tout acte par lequel une personne agissant à titre onéreux met ou promet de mettre des fonds à la disposition d'une autre personne ou prend, dans l'intérêt de celle-ci, un engagement par signature tel qu'un aval, un cautionnement, ou une garantie ».

216. - Art. L. 511-5 CMF.

217. - Art. L. 571-3 CMF.

218. - Le raisonnement mené par l'ACPR n'était pas exempt de défaut. Le prêteur, susceptible de violer le monopole bancaire, n'est pas la plateforme, mais le particulier. L'ACPR en déduisait que la plateforme pourrait être poursuivie comme complice de l'exercice illégal de la profession de banquier (*Guide du financement participatif...*, préc., p. 4). Mais il aurait fallu que certains bailleurs de fond utilisant la plateforme pratiquent les opérations de crédit à titre habituel : l'habitude n'est pas à rechercher chez le complice, mais chez l'auteur principal de l'infraction.

219. - Art. D. 321-1, 1° et 5° CMF.

220. - Art. L. 531-1 s. CMF.

que tous les intervenants du secteur se plient à des règles draconiennes et sont d'une solidité — théoriquement — à toute épreuve. Il ne servirait à rien de concevoir des carcans rigides s'il était possible de s'en échapper sous prétexte d'un exercice discret ou léger de la profession réglementée.

314. **L'adoubement ultérieur du modèle d'entremise** - Mais les autorités ont compris par la suite qu'organiser un face-à-face entre deux publics constituait un métier différent. Une banque reçoit des dépôts des uns et prête aux autres : elle est deux fois partie à un contrat principal, elle est une actrice engagée. Une plateforme de financement participatif suscite une rencontre, puis s'efface.

Une ordonnance a ainsi entrepris d'abaisser méthodiquement l'ensemble des obstacles précédemment décrits²²¹. La solution a consisté notamment dans la création de deux nouvelles professions réglementées, au statut bien plus léger : les intermédiaires en financement participatif et les conseillers en investissement participatif²²². Le premier est ainsi défini : « L'intermédiation en financement participatif **consiste à mettre en relation, au moyen d'un site Internet**, les porteurs d'un projet déterminé et les personnes finançant ce projet dans les conditions suivantes [...] »²²³.

Ainsi, reconnues comme des professionnels de l'entremise, les plateformes de l'économie numérique bénéficient d'un statut distinct, et moins exigeant que celui des acteurs classiques s'impliquant personnellement sur le marché considéré²²⁴. Le même raisonnement peut être transposé aux entremetteurs intervenant sur le marché des transports, de la restauration, de l'hébergement ou des services à la personne.

Mais les faveurs consenties à la plateforme doivent cesser si elle quitte le ciel pour la terre, et qu'elle s'immisce substantiellement dans le fonctionnement de l'économie qu'elle prétend contempler.

221. - Ordonnance n° 2014-559 du 30 mai 2014 relative au financement participatif : P.-H. Conac, « Le nouveau régime du financement participatif », *Rev. sociétés*, 2014, p. 461 ; C. Berrebi et S. Vatin, « Le crowdfunding en pratique, opportunités et limites », *JCP G*, 2014, n° 49, 1266 ; T. Bonneau, « Le financement participatif. - Ord. 30 mai 2014, D. 16 sept. 2014 et AA. 22 et 30 sept. 2014 », *JCP E*, n° 42, 16 oct. 2014, 1523 ; A.-V. Le Fur, « Enfin un cadre juridique pour le crowdfunding, une première étape dans la réglementation », *D.*, 2014, p. 1831.

222. - Les premiers organisent les campagnes de prêts ou de dons. Les seconds gèrent les levées de fonds contre des titres de capital ou de créance.

223. - Art. L. 548-1 al. 1 CMF. Souligné par nous.

224. - En matière de transport routier de personnes, les articles L. 3141-1 et suivants du Code des transports consacrent un titre spécifique au « activités de mise en relation ». Ils sont issus d'une loi n° 2016-1920 du 29 décembre 2016 relative à la régulation, à la responsabilisation et à la simplification dans le secteur du transport public particulier de personnes.

2 – La limite : la direction du marché

315. **Au-delà de l’entremise** – Comment faut-il traiter la plateforme qui dépasse sa fonction de simple mise en relation ? C’est la question posée par une affaire pendante devant la Cour de justice de l’Union européenne, dans laquelle l’avocat général a déjà rendu de riches conclusions²²⁵. En substance, une association professionnelle regroupant des chauffeurs de taxis barcelonais a demandé à une juridiction espagnole de condamner la société Uber à cesser ses activités dans la cité comtale. Selon elle, Uber devrait être considérée comme une société de transport et devrait, à ce titre, justifier de licences sans lesquelles il est interdit d’exploiter un service de taxis à Barcelone²²⁶.

L’avocat général se demande toutefois s’il ne convient pas plutôt de rattacher l’activité de la plateforme californienne à la directive sur les communications électroniques, en tant qu’elle constituerait un « service de la société de l’information »²²⁷. Pour le savoir, il est amené à poser une question plus fondamentale, qui nous intéresse directement :

Qu’est-ce qu’Uber ? Est-ce une entreprise de transport, de taxi pour le dire plus franchement ? Ou bien est-ce uniquement une plateforme électronique permettant de trouver, de réserver et de payer un service de transport presté par autrui ?

(...) Dans ses observations écrites, Uber prétend se limiter uniquement à lier l’offre (de transport urbain) à la demande. Je pense cependant que c’est une vision réductrice de son rôle. En fait, Uber fait beaucoup plus que lier l’offre à la demande : il a lui-même créé cette offre. Il en régleme également les caractéristiques essentielles et en organise le fonctionnement²²⁸.

La démonstration de l’avocat général s’appuie sur plusieurs critères, qui ne sont pas tous d’égale importance.

316. **Le critère du marché nouveau** - D’abord, l’avocat général souligne que la plateforme « a créé l’offre ». Elle se différencierait, en cela, des sites mettant en relation des clients avec des hôtels ou des compagnies aériennes. Ces prestataires ont une activité propre et préexistante, que l’intermédiation ne fait que faciliter, mais ne conditionne pas²²⁹.

225. - Conclusions de l’avocat général M. Maciej Szpunar dans l’affaire *Asociation Profesional Elite Taxi c./ Uber Systems Spain SL*, C-434/15, 11 mai 2017.

226. - Conclusions précitées, §16.

227. - L’article 2, a) de la directive 2000/31/CE du 8 juin 2000 renvoie la définition de cette notion à l’article 1^{er} paragraphe 2 de la directive 98/34/CE du 22 juin 1998 : « (...) tout service presté normalement contre rémunération, à distance par voie électronique et à la demande individuelle d’un destinataire de services ».

228. - Conclusions précitées dans l’affaire C-434/15, § 41 et 43.

229. - Conclusions précitées, §59.

Un tel raisonnement risque toutefois d'englober la grande majorité des plateformes de l'économie numérique. Parce qu'elles permettent une agrégation de micro-acteurs pour former une offre décente, parce qu'elles mobilisent des modèles d'affaires innovants, elles sont souvent à l'origine de l'apparition de marchés entièrement nouveaux. Est-ce incompatible, par la suite, avec une activité de simple entremise ? Pas nécessairement. Avant les plateformes de financement participatif, le marché du micro-don ou du micro-prêt n'existait pas, pour ainsi dire. Cela ne signifie pas que les intermédiaires outrepassent leur rôle et prennent les rênes du marché dont ils ont permis la naissance. Avant qu'un programmeur bienveillant ne lance le site *La machine du voisin*, puis ne s'en désintéresse pour l'essentiel, le marché de la lessive chez l'habitant (offerte, défrayée ou payante) n'existait pas ; pour autant, la plateforme n'exerce aucun contrôle sur ses contours.

Ensuite, l'avocat général relève que l'accès à la plateforme est soumis à conditions : Uber impose ses contrôles aux chauffeurs qui souhaitent proposer leurs services par son intermédiaire. Mais toutes les exigences citées ne sont pas du même ordre. Lorsque la société californienne vérifie qu'un candidat-chauffeur est titulaire du permis de conduire, qu'il est titulaire d'une assurance obligatoire de responsabilité civile et que son véhicule a passé avec succès un contrôle technique, cela revient à vérifier l'aptitude même du prestataire à délivrer le service promis²³⁰. Des vérifications aussi élémentaires ne sont pas incompatibles avec un modèle d'entremise : elles en constituent au contraire un élément nécessaire²³¹.

En revanche, les conclusions mettent en exergue d'autres critères qui, eux, révèlent bien que la plateforme entend imposer autoritairement au marché une direction qu'il n'aurait peut-être pas prise spontanément. Ainsi, Uber encourage les chauffeurs à se rendre dans certaines zones géographiques et à s'y rendre disponibles²³². De plus, plutôt que de s'en remettre à l'offre et à la demande pour déterminer le nombre de courses qu'un chauffeur donné souhaitera proposer chaque jour, elle en fausse le jeu en attribuant des bonus ou des primes aux conducteurs justifiant d'un activisme exceptionnel²³³. Surtout, « (...) c'est Uber qui détermine le prix du service presté. Ce prix est calculé en fonction de la distance et de la durée du trajet, telles qu'enregistrées par l'application à l'aide de la géolocalisation. Un algorithme ajuste ensuite le prix à l'intensité de la demande, en multipliant le prix de base par un facteur approprié dès que la demande augmente à la suite, par

230. - Conclusions précitées, § 44 à 47.

231. - V.infra, n°322.

232. - Conclusions précitées, §47.

233. - Ibid.

exemple, d'un évènement ou simplement d'un changement des conditions météorologiques, tel qu'un orage »²³⁴.

À en croire l'avocat général, la plateforme contrôle par conséquent la nature, la qualité, la disponibilité et le prix du service. Il en conclut qu'Uber ne se contente pas de livrer un « service de la société de l'information », qui aurait constitué en une prestation numérique d'entremise²³⁵. Abandonnant le rôle de simple guide, d'observateur et de commentateur, il prend pied sur le marché considéré et en devient un acteur à part entière. La grille d'analyse ainsi proposée est précieuse, et permettra de faire le départ entre les véritables plateformes d'entremise et les plateformes opérationnelles.

Revenons à celles qui se trouvent dans la première catégorie. Nous avons vu qu'elles se situent hors du marché, ce qui les affranchit de certains devoirs. Mais en se plaçant au-dessus du marché, elles doivent néanmoins être assujetties à certaines obligations.

B – Les plateformes au-dessus du marché : le régime du courtage

317. **Courtages et mandats** – La qualification la mieux adaptée à la majorité des contrats unissant les plateformes numériques à leurs utilisateurs a déjà été suggérée à plusieurs reprises : il s'agit du courtage²³⁶. « [...] le courtier est un coureur contractuel. Il est un commerçant qui, à titre professionnel, rapproche des personnes désireuses de contracter ; un trait d'union entre les parties éventuelles à un contrat, se bornant néanmoins à les rapprocher pour les amener à contracter ensemble, le cas échéant [...]. Il est un intermédiaire dans la conclusion des contrats »²³⁷. Les sites considérés passent généralement sous silence le mot de courtier, voire le rejettent expressément, sans proposer pour autant une autre qualification juridique²³⁸.

234. - Conclusions précitées, §49. L'avocat général précise que le chauffeur est théoriquement libre de fixer le prix de sa course, mais que cette prérogative est destinée à rester purement virtuelle : « (...) si une telle faculté leur est théoriquement accordée, Uber prélève cependant, au titre de commission, le montant qui ressort du calcul du prix du trajet effectué par l'application. Toute éventuelle diminution du prix payé par le passager se ferait au détriment du chauffeur, il est donc peu probable que celui-ci fasse usage de cette faculté » (§50).

235. - Conclusions précitées, §94.

236. - En ce sens, par ex. : N. Mathey, « L'uberisation et le droit des contrats », communication lors du colloque *Le droit civil à l'ère numérique* du 21 avril 2017, Université Panthéon-Assas.

237. - N. Dissaux, V° « Courtage » in *Rép. commercial Dalloz*, avril 2017, n° 1.

238. - AirBnB par exemple, précise dans ses conditions générales qu'il n'est pas « courtier immobilier » (art. 1.2) mais se qualifie de « place de marché en ligne » (art. 1.1), ce qui ne renvoie pas à une qualification juridique précise (conditions générales du 19 juin 2017).

Lorsqu'une des parties souhaite que la plateforme passe des actes juridiques en son nom et pour son compte, un contrat de mandat peut accompagner ou remplacer le courtage²³⁹. Ainsi l'intermédiaire en covoiturages BlaBlaCar exige-t-il dans ses conditions générales de bénéficier d'un mandat d'encaissement, qui lui permet de recevoir lui-même le prix du voyage : le courtier devient de surcroît mandataire ponctuel²⁴⁰. Lorsque la plateforme est chargée plus largement de conclure le contrat sous-jacent, au nom et pour le compte de l'un de ses deux usagers, le courtage cède entièrement la place au mandat : c'est par exemple le cas en matière de réservation hôtelière en ligne²⁴¹.

C'est donc un paysage de courtages — mêlé de mandats — qui s'offre à celui qui contemple l'univers des intermédiaires numériques. La qualification éclaire le régime de ces services, s'agissant notamment de deux difficultés d'une importance pratique considérable : la mise en évidence d'éventuels conflits d'intérêts affectant la plateforme (1), et l'intensité du conseil attendu d'elle s'agissant de l'adéquation des offres aux demandes (2).

1 – Les informations relatives à la plateforme

318. L'indépendance de l'intermédiaire – Le rapport Terrasse affirmait que « (...) réguler le rôle prescripteur des plateformes porte un double enjeu. Pour le consommateur, le recours à des places de marché numériques doit effectivement permettre de bénéficier d'une grande liberté de choix dans des conditions d'information et de transparence idoines. Pour les utilisateurs offreurs, l'équilibre dans la relation avec la plateforme doit garantir l'exercice d'une concurrence loyale »²⁴².

Le courtier se présente comme un professionnel indépendant, dispensant des conseils impartiaux et se plaçant toujours au service du meilleur intérêt de ceux qui le consultent. Mais ce service perd tout sens si l'intermédiaire passe des accords secrets avec des acteurs de marché pour orienter les foules, par priorité, vers leurs offres de contrats ; s'il vend son indépendance prétendue au plus offrant, et bat monnaie de la confiance trahie.

239. - Cette affirmation n'a de sens que dans le paradigme classique, qui présente mandat et courtage comme deux figures parfaitement distinctes. Un auteur estime qu'en réalité, le courtage est une espèce du genre plus large que constitue le mandat (N. Dissaux, V° « Courtage », art. préc., n° 40 et s.)

240. - Article 5.4.1 : « En utilisant la Plateforme en tant que Conducteur pour des Trajets avec Réservation, vous confiez à BlaBlaCar un mandat d'encaissement du montant de la Participation aux Frais en votre nom et pour votre compte [...] » (conditions générales du 19 mai 2017).

241. - Art. L. 311-5-1 al. 1 du Code du tourisme : « Le contrat entre un hôtelier et une personne physique ou morale exploitant une plateforme de réservation en ligne portant sur la location de chambres d'hôtel aux clients ne peut être conclu qu'au nom et pour le compte de l'hôtelier et **dans le cadre écrit du contrat de mandat** mentionné aux articles 1984 et suivants du code civil » (souligné par nous).

242. - P. Terrasse (dir.), *Rapport au Premier ministre sur l'économie collaborative*, précité, point 2.2.2.

Le droit du courtage n'a pas attendu les technologies numériques pour tenir compte de ces dangers. La loi régissant les intermédiaires d'assurance en fournit un exemple frappant :

Avant la conclusion d'un premier contrat d'assurance, l'intermédiaire(...) doit fournir au souscripteur éventuel des informations relatives (...) le cas échéant, à l'existence de liens financiers avec une ou plusieurs entreprises d'assurance.

II. – Avant la conclusion de tout contrat, l'intermédiaire doit : [...]

c) S'il n'est pas soumis à une obligation contractuelle de travailler exclusivement avec une ou plusieurs entreprises d'assurance et qu'il se prévaut d'un conseil fondé sur une analyse objective du marché, il est tenu d'analyser un nombre suffisant de contrats d'assurance offerts sur le marché, de façon à pouvoir recommander, en fonction de critères professionnels, le contrat qui serait adapté aux besoins du souscripteur éventuel [...] »²⁴³.

Le monde du numérique et celui de l'assurance se rejoignent d'ailleurs, puisqu'il existe des comparateurs en ligne de produits assurantiels. Une directive récente les a expressément soumis aux mêmes règles que les intermédiaires classiques²⁴⁴.

319. **La « loyauté » des plateformes** – Les textes récemment adoptés en contemplation des nouveaux intermédiaires numériques ne font donc, au mieux, que remettre au goût du jour des questions aussi vieilles que le contrat de courtage. Après avoir défini la « plateforme en ligne », le Code de la consommation fait ainsi peser sur elle des obligations visant à protéger la confiance que le public place en sa neutralité²⁴⁵.

Tout opérateur de plateforme en ligne est tenu de délivrer au consommateur une information loyale, claire et transparente sur :

1° Les conditions générales d'utilisation du service d'intermédiation qu'il propose et sur les modalités de référencement, de classement et de déréférencement des contenus, des biens ou des services auxquels ce service permet d'accéder ;

243. - Article L. 520-1 du Code des assurances (souligné par nous).

244. - Directive 2016/97 du 20 janvier 2016 sur la distribution d'assurance, art. 2 : « 1. Aux fins de la présente directive, on entend par : (...) "distribution d'assurances", toute activité consistant à fournir des conseils sur des contrats d'assurance, à proposer des contrats d'assurance ou à réaliser d'autres travaux préparatoires à leur conclusion, à conclure de tels contrats, ou à contribuer à leur gestion et à leur exécution, notamment en cas de sinistre, y compris la fourniture d'informations sur un ou plusieurs contrats d'assurance selon des critères choisis par le client sur un site Internet ou par d'autres moyens de communication et l'établissement d'un classement de produits d'assurance comprenant une comparaison des prix et des produits [...] » (souligné par nous).

245. - La définition figure à l'article L. 111-7, I C. conso. : « Est qualifiée d'opérateur de plateforme en ligne toute personne physique ou morale proposant, à titre professionnel, de manière rémunérée ou non, un service de communication au public en ligne reposant sur : 1° Le classement ou le référencement, au moyen d'algorithmes informatiques, de contenus, de biens ou de services proposés ou mis en ligne par des tiers ; 2° Ou la mise en relation de plusieurs parties en vue de la vente d'un bien, de la fourniture d'un service ou de l'échange ou du partage d'un contenu, d'un bien ou d'un service ».

2° L'existence d'une relation contractuelle, d'un lien capitalistique ou d'une rémunération à son profit, dès lors qu'ils **influencent le classement ou le référencement** des contenus, des biens ou des services proposés ou mis en ligne (...) ²⁴⁶.

Un décret a décliné les modalités pratiques de ces devoirs²⁴⁷. On ne comprend pas, toutefois, pourquoi ceux-ci sont limités à l'existence d'une relation de consommation. Par comparaison, le Code des assurances commande aux courtiers de faire preuve de transparence à l'égard de tout souscripteur. L'appartenance à la catégorie des professionnels implique éventuellement une certaine compétence à l'égard du bien ou service faisant l'objet du contrat intermédié, mais elle n'offre aucune connaissance magique des secrets de la plateforme que sont le fonctionnement intime de ses algorithmes, ou l'existence d'accords commerciaux de nature à privilégier certaines offres au détriment d'autres. De plus, comme le relèvent des auteurs, les professionnels sont intéressés par ces informations non seulement lorsqu'ils recherchent des contenus, mais aussi lorsqu'ils en proposent : « (...) ils sont le plus souvent en situation de dépendance à l'égard de ces nouveaux chefs de file et peuvent subir de plein fouet leurs changements de critères de classement ou de référencement ; ils peuvent même, parfois, se trouver en situation de concurrence avec ces nouveaux prescripteurs (ou ceux-ci se trouvent souvent en capacité de s'interposer) »²⁴⁸.

Un texte distinct a été consacré aux comparateurs en ligne de biens et services, qui doivent « (...) apporter une **information loyale, claire et transparente**, y compris sur ce qui relève de la publicité [...] »²⁴⁹.

À ces premiers dispositifs s'ajoute un texte destiné à lutter contre les faux avis de clients.

320. La fiabilité des avis de clients – La manière dont la plateforme agence les résultats de recherche n'est pas le seul paramètre susceptible d'influer sur les décisions de ceux qui les

246. - Art. L. 111-7, II C. conso (souligné par nous), issu de la loi précitée n° 2016-1321. L'article L. 117-7-1 al. 1 du même Code prévoit que les opérateurs de plateformes dont l'activité dépasse un seuil de connexions fixé par décret « (...) élaborent et diffusent aux consommateurs des bonnes pratiques visant à renforcer les obligations de clarté, de transparence et de loyauté [...] ». L'alinéa 2 prévoit que : « L'autorité administrative compétente peut procéder à des enquêtes (...) afin d'évaluer et de comparer les pratiques des opérateurs de plateformes en ligne [...] ». Sur ce texte : J. Rochfeld et C. Zolynski, « La "loyauté" des "plateformes". Quelles plateformes ? Quelle loyauté ? », *Dalloz IP/IT*, 2016, p. 520 ; J. Sénéchal, « Ubérisation et droit de la consommation », *Dalloz IP/IT*, 2017, p. 363.

247. - Art D. 111-6 et s. du Code de la consommation, issu du n° 2017-1434 du 29 septembre 2017 relatif aux obligations d'information des opérateurs de plateformes numérique.

248. - J. Rochfeld et C. Zolynski, « La "loyauté" », art. préc. Les auteurs précisent : « Il aurait donc été bienvenu d'instituer une obligation d'information dans ces rapports B to B, portant sur toute "modification importante de leurs politiques tarifaires, leurs politiques de contenus, d'accès aux API ou de changements substantiels dans les critères de classements des algorithmes" Cette extension, un temps envisagée, a finalement été écartée à l'occasion des débats parlementaires ». La citation intercalée est issue de l'avis précité du Conseil national du numérique sur la loyauté des plateformes.

249. - Art. L. 111-6 C. conso. Nous soulignons.

consultent. C'est aujourd'hui une pratique presque universellement répandue que d'offrir aux acheteurs de biens ou utilisateurs des services sous-jacents la possibilité de leur attribuer une note de satisfaction. Ces informations s'agrègent à celles qui figurent à la plateforme pour former, dans l'esprit de celui qui la consulte, un tout cohérent. Le rapport Terrasse insiste sur l'influence manifeste de ces avis de consommateurs :

Le baromètre 2015 de l'institut Opinion Way sur le commerce entre internautes révèle que 74% d'entre eux considèrent que la possibilité de noter les acheteurs et les vendeurs est un élément fondamental de l'instauration de la confiance dans ce type de relation. Le baromètre 2014 révélait que 74% ont déjà renoncé à acheter un produit à cause de commentaires ou d'avis négatifs. Le système de notation, son ergonomie, sa pertinence au regard de l'activité conduite, sa fiabilité, sont un facteur clef de fréquentation pour la plateforme et de différenciation par rapport à ses concurrentes²⁵⁰.

Organiser des campagnes de faux avis, injustement critiques ou laudateurs, constitue donc pour la plateforme, pour le fournisseur du bien ou du service, pour des concurrents ou pour des tiers, un moyen simple et efficace de faire fuir ou d'attirer des foules de clients. Pour prévenir ces risques, le Code de la consommation prévoit les mesures suivantes :

(...) toute personne physique ou morale dont l'activité consiste, à titre principal ou accessoire, à collecter, à modérer ou à diffuser des avis en ligne provenant de consommateurs est tenue de délivrer aux utilisateurs une information loyale, claire et transparente sur les modalités de publication et de traitement des avis mis en ligne.

Elle précise si ces avis font ou non l'objet d'un contrôle et, si tel est le cas, elle indique les caractéristiques principales du contrôle mis en œuvre.

Elle affiche la date de l'avis et ses éventuelles mises à jour.

Elle indique aux consommateurs dont l'avis en ligne n'a pas été publié les raisons qui justifient son rejet.

Elle met en place une fonctionnalité gratuite qui permet aux responsables des produits ou des services faisant l'objet d'un avis en ligne de lui signaler un doute sur l'authenticité de cet avis, à condition que ce signalement soit motivé²⁵¹.

Ces mesures n'ont donc pas pour objet principal de contraindre les centrales d'avis à produire une information plus fiable. Elles doivent simplement afficher des informations qui constituent autant d'indices de leur crédibilité ou, au contraire, de leur manque de sérieux²⁵².

250. - P. Terrasse (dir.), rapport précité, point 2.2.2. A propos du sondage cité, il est précisé que « Le Baromètre du C to C PriceMinister/La Poste/OpinionWay 2015 est une étude quantitative réalisée auprès d'un échantillon de 1051 personnes, représentatives de la population des internautes français âgés de 15 à 69 ans, selon les critères de sexe, d'âge, de CSP de la personne interrogée, de région et de taille d'habitat. Le questionnaire a été administré du 22 au 30 septembre 2015. L'édition 2015 est la dixième édition » (note 99, p. 33).

251. - Art. L. 111-7-2 C. conso., issu de la loi n° 2016-1321 précitée.

252. - Cette philosophie générale est déclinée en détail par les articles D. 111-16 et suivants du Code de la

Ainsi, si le statut d'intermédiaire est plus léger que celui d'acteur du marché sous-jacent, il n'en est pas pour autant dénué d'obligations. Après avoir informé ses utilisateurs sur son propre fonctionnement, la plateforme doit renseigner suffisamment sur les caractéristiques des contrats dont elle propose la conclusion.

2 – Les informations relatives au contrat projeté

321. Le courtage classique : un contrôle de faisabilité assorti d'un conseil personnalisé – On considère traditionnellement que le courtier doit délivrer à celui qui sollicite ses conseils des renseignements suffisants sur le contrat envisagé. Ils portent à la fois sur le partenaire potentiel, et sur l'objet de l'éventuelle convention.

Le courtier doit en premier lieu présenter à son client son futur cocontractant, ce qui justifie de vérifier son existence d'abord, son identité ensuite, sa capacité apparente à exécuter ses obligations enfin²⁵³.

Il doit en second lieu présenter les contours du bien ou service dont il propose l'achat, ce qui suppose d'en expliquer le fonctionnement s'il est complexe, et de justifier en toute hypothèse en quoi il correspond aux besoins du client. À nouveau, le courtage en assurances en fournit une très claire illustration. L'intermédiaire doit :

2° Préciser les exigences et les besoins du souscripteur éventuel ainsi que les raisons qui motivent le conseil fourni quant à un produit d'assurance déterminé. Ces précisions, qui reposent en particulier sur les éléments d'information communiqués par le souscripteur éventuel, sont adaptées à la complexité du contrat d'assurance proposé²⁵⁴.

La procédure ainsi conçue repose sur un dialogue entre le courtier et son client, visant à adapter et à personnaliser autant que possible le conseil prodigué.

Les attentes sont-elles aussi fortes à l'égard des nouveaux intermédiaires numériques ?

consommation, issus d'un décret n° 2017-1436 du 29 septembre 2017 relatif aux obligations d'information relatives (sic) aux avis en ligne de consommateurs. Par exemple, aucune procédure de contrôle des avis n'est rendue obligatoire ; le principe d'un avis fourni moyennant contrepartie n'est pas prohibé (art. D. 111-7 C ; conso.). Il suffit à l'organisateur des avis d'afficher sa politique sur ces questions.

253. - N. Dissaux, V° « Courtage », art. préc., n° 131 s. Sur la nécessité de vérifier que le partenaire présenté existe bel et bien : Cass. com., 8 janvier 1991, n° 88-16.808 : « (...) l'arrêt a retenu à bon droit qu'il incombait à la société Incosa, en sa qualité de courtier professionnel dont le rôle consiste à mettre le donneur d'ordre en mesure de contracter, de garantir l'identité de l'autre partie ; qu'ayant constaté qu'elle avait proposé à la Scari un acheteur qui n'existait plus, peu important la façon dont il avait disparu et le sort de son patrimoine, la cour d'appel a pu considérer que la société Incosa avait commis une faute et devait réparation du préjudice subi (...) ».

254. - Art. L. 520-1, II du Code des assurances.

322. **Le courtage numérique : un contrôle superficiel ?** - Mobilisons une fois encore l'exemple du financement participatif, qui fait l'objet d'une réglementation complète et récente.

La loi fait naturellement obligation à un intermédiaire en financement participatif — celui qui s'occupe d'une opération de don ou de prêt participatif — de fournir les principales caractéristiques objectives de l'opération projetée : s'agissant d'un crédit par exemple, le taux doit être indiqué, le montant total ou encore la durée du prêt²⁵⁵. C'est bien la moindre des choses.

La plateforme procède-t-elle à une vérification au moins élémentaire du sérieux et de la cohérence des projets proposés aux bailleurs de fonds ? La loi est ici d'une sobriété étonnante, puisque les intermédiaires doivent seulement « Informer le public des conditions de sélection des projets et des porteurs de projet », ce qui n'interdit en rien le laxisme, mais oblige seulement à l'afficher²⁵⁶. Une société du secteur présente ainsi sa politique de sélection :

*Aux fins d'être accepté par la Société pour la promotion éventuelle sur le Site, le Porteur de Projets s'engage à fournir de manière claire et précise, pour tout Projet proposé (...). Les caractéristiques et paramètres du Projet sont soumis à l'acceptation préalable de la Société sans obligation de motiver son refus et sans garantir en rien le Ululer sur la réussite du Projet ou l'authenticité des informations présentées par le Porteur de Projet. En effet, la sélection des contenus vise essentiellement à vérifier la cohérence et la qualité du Projet **et n'a pas pour objet de contrôler la viabilité, la faisabilité** ou l'authenticité du Projet proposé.*

À titre d'exemple, la Société refusera de manière systématique les Projets fantaisistes, dénués de sérieux, détachés de toute réalité concrète et voués à l'échec²⁵⁷.

Jamais on n'admettrait d'un courtier en assurance qu'il se dispense de tout contrôle de « faisabilité » de l'opération projetée.

Ces moindres exigences face aux intermédiaires numériques peuvent s'expliquer. Nous avons présenté leur haut degré d'automatisation comme une condition de leurs faibles coûts de transaction. C'est ce qui permet de les utiliser pour de petites opérations et, par voie de conséquence, c'est ce qui ouvre les nouveaux marchés consistant à agréger des armées de micro-professionnels ou d'amateurs. Le financement participatif obéit parfaitement à cette logique. Or, plus le niveau de contrôle attendu de la plateforme augmente, plus elle doit renchérir sa commission

255. - Art. L. 548-6, 4° CMF : ces intermédiaires doivent « Fournir aux prêteurs ou donateurs les informations concernant les caractéristiques du projet et, le cas échéant, du prêt concerné s'agissant en particulier du taux d'intérêt applicable, du montant total du crédit, de la durée du prêt, de ses modalités et conditions de remboursement ainsi que de l'existence ou non d'une faculté de rétractation du prêteur ».

256. - Art. L. 548-6, 2° CMF.

257. - Conditions générales Ulule, point 3.2 « Présentation des projets » (7 septembre 2017). A titre de comparaison, les conditions générales du géant du secteur, Kickstarter, ne formulent aucun critère de sélection, violant par conséquent les exigences pourtant minimales de l'ordonnance française (version du 19 octobre 2014).

et même — pour éviter d’engager sa responsabilité civile — resserrer sa sélection, au risque de se substituer aux internautes dans le choix des projets à soutenir. De surcroît, contrôler la solidité et le sérieux de ces foules de petits acteurs est bien plus difficile que de vérifier, pour un courtier en financement ou en assurance, qu’il a bien affaire à un établissement de crédit ou un assureur agréé.

Les mêmes difficultés se retrouvent au stade du conseil sur les caractéristiques du produit présenté et son adéquation aux besoins de l’utilisateur.

323. Le courtage numérique : un conseil standardisé ? - Revenons à la loi applicable aux intermédiaires en financement participatif. Ils doivent « Mettre en garde les prêteurs sur les risques liés au financement participatif de projet, notamment les risques de défaillance de l’emprunteur, et des porteurs de projets sur les risques d’un endettement excessif »²⁵⁸.

Ainsi formulé, le texte semble exiger une mise en garde abstraite contre les risques généraux présentés par toute opération de financement participatif. Là encore, il est possible que les coûts engendrés par des avertissements personnalisés aient semblé dissuasifs aux rédacteurs de l’ordonnance.

S’agissant des « conseillers en investissement participatif » — qui s’occupent des prises de participation en capital par une foule de petits investisseurs —, les attentes semblent cependant plus élevées. Ils doivent : « S’enquérir auprès de leurs clients ou de leurs clients potentiels de leurs connaissances et de leur expérience en matière d’investissement ainsi que de leur situation financière et de leurs objectifs d’investissement, de manière à s’assurer que l’offre proposée est adaptée à leur situation [...] »²⁵⁹.

Les collectes de fonds participatives sont des opérations de plus grande ampleur, qui s’accommodent de coûts de transaction plus élevés. Elles permettent de consacrer davantage de ressources humaines à chaque opération. Toutefois, le texte semble compatible avec une large part d’automatisation : un questionnaire en ligne permettra de cerner le profil de l’investisseur, et de le diriger vers des projets plus ou moins spéculatifs, classés par catégories.

Le risque existe donc que ces nouveaux courtiers se livrent à des sélections laxistes des biens et services proposés sur leur plateforme, accompagnées de conseils automatisés et non véritablement personnalisés. Les intermédiaires sont débiteurs d’obligations moins intenses, et leur responsabilité pourra plus rarement être recherchée que dans l’univers « hors-ligne ».

258. - Art. L. 548-6, 5° CMF.

259. - Art. L. 547-9, 6° CMF.

De ce point de vue, le mouvement qui souhaite accentuer la tendance jusqu'à faire disparaître les intermédiaires est susceptible d'inquiéter.

324. L'avenir : une disparition complète de certains intermédiaires ? - Certains imaginent se fonder sur les technologies des *blockchains* et des *smart contracts* pour organiser la rencontre en ligne d'une offre et d'une demande sans passage par un intermédiaire centralisé. Parmi les projets de ce type, l'un des plus connus actuellement se nomme Arcade City²⁶⁰. Créé par des déçus d'Uber, il doit permettre à des passagers et à des chauffeurs de négocier directement le prix d'une course, et de figer l'accord ainsi obtenu dans une chaîne de blocs. Un *smart contract* branché sur des moyens de paiement et un module de géolocalisation en assurera l'exécution.

Il est sans doute trop tôt pour dire si ce modèle de « plateforme » décentralisée et sans opérateur est réaliste. On imagine qu'il faut bien des opérateurs centraux pour vérifier l'aptitude des candidats-chauffeurs, mais il existe ou existera un jour un moyen automatisé de prouver que l'on est titulaire du permis de conduire. On songe ensuite qu'il faut un mécanisme centralisé quelconque pour qu'une commission soit perçue par les fondateurs, qui n'auront pas toujours créé les outils dans le seul but d'être utiles à leur prochain. Mais les fondateurs d'Arcade City semblent avoir imaginé un modèle dont le fonctionnement se détache en quelques années de son noyau originel, après avoir assuré à ses créateurs une confortable rétribution²⁶¹. Admettons que tous ces obstacles soient surmontés et qu'un fonctionnement véritablement décentralisé se dessine : les dernières traces de conseil, de contrôle et de responsabilité civile associées aux nouveaux intermédiaires disparaissent alors. Ainsi, dans certains domaines, on aurait assisté à la transformation d'un acteur de marché opaque, personnellement partie aux transactions, en un courtier translucide, avant que ne se produise une évaporation totale des intermédiaires.

À présent qu'une vision du présent et du futur de l'intermédiation numérique a été proposée, il nous faut pour finir évoquer son influence sur les conventions sous-jacentes.

II – Les contrats intermédiés

325. Une remise en cause des modèles asymétriques – Dans un paradigme capitaliste classique, l'unité économique la plus puissante n'est pas le simple intermédiaire, mais l'acteur de marché. Les relations contractuelles qu'elle entretient avec son écosystème sont marquées par une

260. - <http://arcade.city>. Sur ce projet, V. par ex. R. Prudent, « Arcade City : l'appli qui rêve d'ubériser Uber », article *tempsreel.nouvelobs.com* du 18 février 2016.

261. - « Arcade-city, le Uber-killer de la blockchain ? », article *blockchainfrance.net* du 19 mars 2016 qui évoque, « à terme, un service public (sic) détenu à 100 % par ses utilisateurs ».

certaine verticalité. D'une part, pour assurer sa production de biens ou de services, elle mobilise des ressources humaines, qui sont placées à son service permanent par une relation de salariat. D'autre part, lorsqu'elle interagit avec sa clientèle — si celle-ci n'est pas elle-même constituée de professionnels — elle exerce fréquemment un pouvoir d'une autre nature, liée à sa plus grande compétence, ainsi qu'à sa capacité à imposer des conventions de masse dont elle a assuré seule la rédaction. Le droit des contrats a pris acte de ces déséquilibres, et secrété des branches spéciales, tout entières pensées pour compenser les asymétries et aménager la faiblesse. Il s'agissait dans le premier cas du droit du travail, dans le second du droit de la consommation. Il n'y restait rien ou presque du postulat d'égalité des parties qui transpirait du Code Napoléon.

Le « capitalisme de plateforme », s'il ne met pas à terre ces constructions, les dérange et les bouscule pour le moins. L'intermédiaire, qu'il soit courtier ou mandataire, est juridiquement transparent. Il ne prend aucune part à la relation fondamentale, celle qui s'instaure entre les parties rapprochées. Dès lors, l'intermédiaire dispose certes de ses propres salariés pour assurer sa mission de traitement de l'information, mais le service recherché au titre du contrat de base peut être assuré par des milliers de professionnels isolés. Ils ne seront plus nécessairement liés entre eux par leur appartenance juridique à de gros blocs de capital appelés « entreprises », qui leur devront en contrepartie des rémunérations stables et une protection sociale : leur point commun sera leur présence dans un catalogue de courtage. L'atomisation des professionnels favorise ainsi la prolifération des statuts de travailleurs indépendants. C'est, en quelque sorte, le stade ultime de l'externalisation. Quant au « client », dans le modèle appelé « économie collaborative », il peut se retrouver face à un fournisseur de bien ou de service amateur, agissant par désœuvrement, conviction ou volonté d'arrondir ses fins de mois. La nouvelle peut sembler bonne au premier abord : elle sonne comme un retour des conventions entre égaux. Mais le client ne perd-il pas les avantages qui sont habituellement ceux d'une relation asymétrique, notamment le bénéfice d'un conseil personnalisé, et la possibilité d'actionner un responsable solvable ou assuré en cas de mauvaise exécution ? Corrélativement, le fournisseur d'un jour est-il vraiment capable d'assumer les engagements qu'il a pris ?

En somme, nous assistons à une remise en cause d'équilibres délicats en matière de travail (A) et de consommation (B).

A – La remise en cause du contrat de travail

326. **Plan** – Comme le relève le Conseil d’État, la modification du paysage économique consécutive à l’essor du capitalisme plateforme n’est pas une vue de l’esprit, mais d’ores et déjà une réalité mesurable.

(...) le processus de déstructuration des formes traditionnelles d’exercice des activités économiques que constitue l’« ubérisation » se traduit de manière globale par la pérennisation de ce que l’organisation internationale du travail (OIT) qualifie d’emploi « atypique » c’est-à-dire l’emploi selon d’autres formes que le contrat de travail à durée indéterminée à temps plein. Et même si parmi ces formes d’emploi atypiques se trouvent notamment celles qui correspondent à un travail à durée déterminée ou à temps partiel, l’OIT a constaté une augmentation sensible au cours des dernières années des formes d’emploi caractéristiques de celles que l’on trouve sur les plateformes numériques de mise en relation²⁶².

La conséquence de ce mouvement est décrite par le Conseil national du numérique en termes inquiétants : « (...) dès lors que le cadre institutionnel assimile l’emploi au travail salarié, le reste des formes d’emploi est exclu de la régulation classique, si bien que la multiplication des régimes, statuts, et modes de contractualisation entraîne le détricotage du salariat [...] »²⁶³.

Les nouvelles formes d’activité (1) pourraient appeler de nouvelles formes de protection (2).

1 – De nouvelles formes d’activité

327. **Le « digital labor »** - Certains auteurs, principalement économistes ou sociologues, ont une vision très englobante de ce qui constitue les nouvelles formes de travail liées aux technologies numériques, qu’ils appellent « *digital labor* ».

Par digital labor, nous désignons les activités numériques quotidiennes des usages des plateformes sociales, d’objets connectés ou d’applications mobiles. Néanmoins, chaque post, chaque photo, chaque saisie et même chaque connexion à ces dispositifs remplit les conditions évoquées dans la définition : produire de la valeur (appropriée par les propriétaires des grandes entreprises technologiques), encadrer la participation (par la mise en place d’obligations et contraintes contractuelles à la contribution et à la coopération contenues dans les conditions générales d’usage), mesurer (moyennant des indicateurs de popularité, réputations, statut, etc.)²⁶⁴.

262. - Conseil d’État, *Puissance publique et plateformes numériques : accompagner l’« ubérisation »*, étude annuelle 2017, p. 84, citant le rapport de l’OIT *Non-Standard Employment around the World. Understanding challenges, shaping prospects*.

263. - CNNum, rapport *Travail, emploi, numérique. Les nouvelles trajectoires*, janvier 2016, p. 34.

264. - A. Casilli et D. Cardon, *Qu’est-ce que le digital labor ?*, INA, 2015, partie « Digital labor : travail, technologies et conflictualités ». M. Casilli, auteur du passage cité, est un promoteur du concept de digital labor, que M. Cardon critique. Leurs contributions au sein de l’ouvrage se répondent.

Ce courant doctrinal s'intéresse donc à des activités qui ne sont pas perçues par celui-là même qui les accomplit comme du travail. L'essentiel est selon eux que l'internaute intègre — inconsciemment — une force collective de production, que les plateformes vont mettre au service de la création d'une valeur économique qui peut être gigantesque, sans jamais la rémunérer²⁶⁵. Celui qui poste une photo sur Facebook crée de la valeur pour cette entreprise, de même que celui qui la « tague » — en y ajoutant manuellement les noms des personnes qu'il identifie —, de même encore que celui qui clique sur « j'aime » — signalant au réseau social que ce contenu éveille l'intérêt. Cela revient en partie à dénoncer l'économie contractuelle spécifique « service contre données personnelles », qui a déjà été abordée²⁶⁶. Mais au-delà, M. Casilli vise « (...) le droit à une rémunération de ce travail ». Cette rémunération, précise-t-il, ne prendrait pas la forme d'un paiement correspondant à la valeur économique de la micro-contribution — qui n'excéderait pas quelques centimes — mais il y voit plus fondamentalement une justification politique à la mise en place d'un revenu universel²⁶⁷.

328. Les tâcherons du numérique – Dans les exemples qui viennent d'être mobilisés, les internautes accomplissent une multitude de tâches très simples, créatrices de valeur lorsqu'elles sont considérées à grande échelle, sans même en avoir conscience. Mais il existe une plateforme proposant d'accomplir des gestes semblables, cette fois-ci sur instruction d'entreprises et contre rémunération : Amazon Mechanical Turk (mTurk)²⁶⁸. Les contreparties sont misérables : « Transcrire une vidéo de 35 secondes, 5 cents. Écrire la description commerciale d'un produit, 12 cents. Noter des photos d'hommes pour un site de rencontres, 3 cents. Répondre à une étude

265. - V. aussi T. Tierranova, « Free labor : producing culture for the digital economy », *Social Text*, 63 (Volume 18, Number 2), Summer 2000, p. 33.

266. - Certains tâches sont cependant accomplies hors d'un cadre contractuel. L'exemple du « CAPTCHA » est célèbre. Pour éviter que leurs zones de commentaires soient envahies par des messages publicitaires postés par des robots, de nombreux sites Internet ont recours à ce test, conçu par Google, qui vise à vérifier que le visiteur est bien humain (l'acronyme signifie *Completely Automated Turing test to Tell Computers and Humans Apart*). Le visiteur est invité à identifier les images contenant une voiture, ou une façade de magasin, ou à déchiffrer un symbole peu lisible. Les réponses fournies servent à entraîner les intelligences artificielles de Google, ce qui produit de la valeur pour l'entreprise.

267. - « (...) la rémunération individuelle des données et des contenus enferme les usagers dans une logique d'atomisation sociale qui n'est pas en accord avec la nature "commune" de ce travail numérique. (...) chez moi, elle prend la forme, non d'un salaire individuel qui dédommagerait les données perdues par l'individu, mais au contraire d'un revenu universel en accord avec la nature collective des activités valorisantes de l'économie numérique. Le fait de proposer un revenu de base inconditionnel serait à la fois un moyen de sortir le digital labor de ce cadre d'activité privée, de donner du pouvoir aux utilisateurs face à des entités plus puissantes qu'eux, et également de reconnaître la nature commune de ce travail et de ses fruits » (A. Casilli et D. Cardon, *Qu'est-ce que le digital labor*, op. cit., partie « débat »).

268. - « Au XVIIIe siècle, le "truc mécanique" était un faux automate joueur d'échecs, qui était en fait activé par un joueur humain. Amazon a aussi recours à des opérateurs humains, plus précisément à des foules de travailleurs flexibles qui "aident les machines" » (*ibid.*, partie « Digital labor : travail, technologies et conflictualités »).

scientifique, 10 cents »²⁶⁹. Le revenu horaire moyen d'un « turker » serait de l'ordre de 2,30 dollars²⁷⁰.

Nous évoquions précédemment une production inconsciente de valeur, vécue comme un instant de loisir. Il s'agit à présent d'un comportement adopté sur ordre — fût-il donné par une hiérarchie désincarnée — et pour un salaire — fût-il misérable. La différence de nature est nette²⁷¹. On ressuscite ici la figure du tâcheron, cet ouvrier peu qualifié payé non pas au mois ou à la semaine, mais à la tâche accomplie. Le constat s'impose davantage encore si l'on considère les plateformes de micro-travail « hors-ligne ». Puisque le « turker » mime les gestes qui sont ceux d'une navigation en ligne classique, l'illusion peut flotter un instant qu'il n'est pas en train d'accomplir un travail. L'exemple de TaskRabbit rétablit la vérité. Les micro-tâches en question consistent à faire les courses pour quelqu'un, à monter un meuble, à porter des objets lourds²⁷². Le cousinage avec la conception traditionnelle du travail est plus flagrant, mais la réalité est au fond exactement la même que dans le cas de mTurk.

Les chauffeurs Uber sont eux aussi payés à la tâche, mais le contexte est quelque peu différent. On peut considérer, comme l'avocat général de la Cour de Justice de l'Union européenne, que c'est bien Uber qui détermine les conditions de l'activité, en orientant les conducteurs vers certains lieux et certaines plages horaires à l'aide de bonus, ainsi qu'en fixant — de fait — le prix de la course²⁷³. Un quasi-employeur stable peut alors être identifié, qui propose lui-même ses prestations à des clients. Dans le cas de mTurk, Amazon joue véritablement un rôle de plateforme. Ce sont les entreprises tierces qui définissent les tâches à accomplir, ainsi que la rémunération qui y est associée. mTurk apparaît comme une agence d'intérim numérique, qui permet à un individu la conclusion de dizaines de micro-contrats de travail quotidiens. Le labeur continu du salariat ordinaire est réduit en miettes, et ces miettes sont jetées sur un petit peuple de prétendus indépendants.

Toutefois, il ne sera pas toujours facile de proposer une analyse tranchée des modèles de travail en cause. Sur certaines plateformes, une liberté d'organisation plus importante reconnue aux

269. - G Orain, « Sur Amazon Turk, les forçats du clic », article *lemonde.fr/pixels* du 22 mai 2017.

270. - *Ibid.*

271. - En ce sens, S. Broca, « Travail, communs et digital labour », communication à l'occasion du séminaire *Entreprendre en communs* du 7 juillet 2017. L'auteur estime qu'il est nécessaire de construire des sous-catégories plus cohérentes au sein des activités saisies par les théoriciens du *digital labor*.

272. - V. la page d'accueil de *taskrabbit.com*.

273. - V. *supra*, n°316.

fournisseurs de biens et services ou un degré d'amateurisme supérieur — réel ou prétendu — contribueront à brouiller les catégories.

La diversité de ces nouveaux modèles appelle à l'évidence une réflexion sur le renouvellement des modes de protection en droit social.

2 – De nouvelles formes de protection

329. **Deux approches** – Si l'on accepte le postulat que la majorité des protections du droit social sont aujourd'hui réservées aux salariés, l'émergence de nouvelles formes d'activités dirigées pose un problème qui peut être résolu de deux manières. La première consiste à repenser ou à assouplir les critères de qualification du contrat de travail, afin que les masses laborieuses du numérique y trouvent refuge. La seconde fait déborder les avantages traditionnellement réservés au salariat au-dehors.

330. **Ramener les nouveaux modèles à l'intérieur du contrat de travail** – La seule solution qui soit à la fois de très court terme et qui se passe de réforme législative consiste à « découvrir » des contrats de travail dans les nouveaux modèles d'organisation issus des plateformes. Un auteur se montre encourageant, soulignant que :

(...) la qualification du contrat de travail est souvent mal comprise. On la croit déterminée uniquement par la subordination, alors qu'elle procède également, en creux, d'une analyse des conditions de l'indépendance. Il a ainsi pu être proposé une analyse renversée du critère du contrat de travail partant, non plus de la subordination, mais des conditions de l'indépendance : le lien de subordination est une qualification négative qui se construit par opposition à celle de l'indépendance. Ainsi, lorsque la qualité juridique d'un prestataire est discutée, et mélange des indices d'indépendance et de subordination, les juges excluent par principe du champ du salariat les vrais indépendants, c'est-à-dire ceux qui disposent à la fois de la maîtrise de leur capacité de profits et des risques inhérents à cette maîtrise. Mais, à l'inverse, lorsque les soi-disant indépendants ne sont pas maîtres de leur capacité de profit, ils doivent être considérés comme des subordonnés. Rapportée aux travailleurs de plateformes, l'absence de clientèle propre apparaît comme un indice essentiel de l'absence d'indépendance. Du coup, et par voie de conséquence, les juges mettent l'accent sur les indices de subordination et reconnaissent l'existence d'un contrat de travail²⁷⁴.

Dans la droite ligne de ce raisonnement, une juridiction californienne a requalifié la relation unissant Uber à l'un de ses chauffeurs en contrat de travail.

Defendants argued that they exercised very little control over Plaintiff's activities. However, the Borello court found that it was not necessary that a principal exercise complete control over a worker's activities in order for that worker to be an employee. « The minimal degree of control that the employer exercised over the details of the work

274. - T. Pasquier, « Le droit social confronté aux défis de l'ubérisation », *Dalloz IP/IT*, 2017, p. 368.

was not considered dispositive because the work did not require a high degree of skill and it was an integral part of the employer's business. The employer was thus determined to be exercising all necessary control over the operation as a whole »²⁷⁵.

Mais il est vrai que le cas d'Uber est de ceux qui se prêtent le mieux à une telle opération de requalification. Cette plateforme, on l'a dit, outrepassa les fonctions traditionnelles du courtier pour prendre les commandes du marché sous-jacent. Elle endosse en réalité un rôle de donneur d'ordres permanent des chauffeurs, instituant avec eux une relation de quasi-salariat. Les concepts traditionnels peuvent l'accueillir au prix d'une légère sollicitation, mais sans exploser. Les modèles de type TaskRabbit ou mTurk ne s'y prêteraient pas de la même façon.

331. Sortir les protections sociales du contrat de travail – Dans son étude annuelle consacrée aux plateformes, le Conseil d'État appelle de ses vœux « le nécessaire dépassement d'une dichotomie devenue trop radicale » entre travail salarié et travail indépendant²⁷⁶. À cet égard, le numérique ne ferait qu'accentuer douloureusement des mouvements amorcés avant et en dehors de lui²⁷⁷. L'enjeu serait alors d'étendre à des non-salariés le bénéfice d'avantages jusqu'ici intimement liés à l'existence d'un contrat de travail. Il ne servirait à rien de préserver un statut puissant et protecteur, si les entreprises s'en évadaient peu à peu jusqu'à ce que personne ou presque n'en bénéficie réellement. Mais abattre la muraille qui sépare ceux qui sont protégés de ceux qui sont nus n'est pas sans risque : dans quel sens l'influence va-t-elle s'exercer ? Le nivellement aura-t-il lieu par le haut ou par le bas ? Supposons qu'un tel décloisonnement soit néanmoins souhaitable et qu'il aboutisse à un export de droits hors du contrat de travail plutôt qu'à leur évaporation. Le champ des bénéficiaires peut être délimité de deux façons : il peut se cantonner à un nouveau groupe des « travailleurs de plateformes », ou s'étendre très largement à toute activité professionnelle, subordonnée comme indépendante²⁷⁸. La « loi travail » de 2016 a investi simultanément ces deux terrains²⁷⁹.

D'une part, la loi a développé une approche spécifique aux intermédiaires numériques. Elle a inséré dans le Code du travail un nouveau titre intitulé : « travailleurs utilisant une plateforme de

275. - Labor Commissioner of the state of California, 16 juin 2015, *Uber Technologies Inc./B. Berwick*. La citation est de California Supreme Court, *S.G. Borello & Sons, Inc. v. Dept. of Industrial Relations* (1989), 48 Cal. 3d 341. Dans le même sens, V. la décision préliminaire londonienne : Employment tribunals, 28 octobre 2016, *Y. Aslam, J. Farrar & others and Uber B.V, Uber London Ltd, Uber Britannia Ltd*.

276. - Conseil d'État, *étude annuelle 2017*, précitée, p. 85.

277. - V. l'exemple du « laveur de carreaux » mobilisé par J.-P. Chauchard, « Les avatars du travail indépendant », *Droit social*, 2009, p. 1065.

278. - Conseil d'État, *étude annuelle 2017*, précitée, p. 88 s.

279. - Loi n° 2016-1088 du 8 août 2016 relative au travail, à la modernisation du dialogue social et à la sécurisation des parcours professionnels.

mise en relation par voie électronique »²⁸⁰. En vertu de ces textes, l'intermédiaire numérique dépassant une certaine taille fixée par décret doit prendre en charge une partie de l'assurance souscrite par le travailleur et couvrant le risque d'accidents du travail, ou encore financer une partie de sa formation professionnelle²⁸¹. Il est également reconnu aux « travailleurs des plateformes » le droit de se syndiquer afin de défendre collectivement leurs intérêts²⁸². Il serait très souhaitable qu'ils le fassent, afin d'atteindre une masse critique leur permettant d'engager des négociations avec la plateforme. Mais encore faut-il qu'ils aient les moyens d'entrer en contact les uns avec les autres, une fonctionnalité qui n'est évidemment pas implémentée spontanément par les grands intermédiaires : la loi ne dit rien de ces détails apparemment anecdotiques, en réalité essentiels.

D'autre part, la « loi travail » a dépassé le problème spécifique du numérique pour faire évoluer la question générale de la protection attachée à l'activité. Elle a pour cela créé un « compte personnel d'activité » qui vise à attacher des droits sociaux, par exemple des droits à formation professionnelle, aux individus plutôt qu'à des situations²⁸³. Qu'il transite par le secteur public ou privé, par le salariat ou l'indépendance, par des périodes d'activité et des périodes de recherche d'emploi, le travailleur emportera sa protection sociale partout avec lui.

M. Pasquier salue ces évolutions destinées à « rendre au droit du travail les atours de son origine : un droit dédié à la protection de toutes les activités de travail »²⁸⁴. Mais il évoque encore une importante question : celle du droit applicable à la rupture, par la plateforme, de sa relation avec le professionnel. Passées les frontières du salariat, le droit du licenciement serait invoqué en vain. L'auteur estime cependant, à juste titre, qu'« Il n'est que de rappeler la récente réforme du droit des obligations — qui a introduit dans le champ du droit commun le contrôle de la violence économique, des clauses abusives, ou encore de la révision pour imprévision — et les dispositions relatives à la rupture des relations commerciales intégrées - article L. 442-6, aliéna 2, du code de commerce -, pour se convaincre du formidable potentiel que recèlent les autres branches du droit pour protéger les travailleurs ubérisés »²⁸⁵.

Les bouleversements des droits spéciaux des contrats entraînés par les nouvelles intermédiations numériques ne se limitent pas au domaine du travail. Ils se constatent encore en droit de la consommation.

280. - Art. L. 7341-1 s. du Code du travail.

281. - Art. L. 7342-2 à L. 7342-4 du Code du travail.

282. - Art. L. 7342-6 du Code du travail.

283. - Art. L. 5151-1 s. du Code du travail.

284. - T. Pasquier, « Le droit social confronté... », art. préc.

285. - *Ibid.*

B – La remise en cause du contrat de consommation

332. **Le problème du face-à-face de particuliers** – Le droit du contrat de consommation, comme celui du contrat de travail, est un droit de protection du faible face au fort. « (...) la relation entre professionnel et consommateur est naturellement déséquilibrée. La compétence du professionnel, les informations dont il dispose, et souvent sa dimension financière lui permettent de dicter sa loi au consommateur »²⁸⁶.

Cette asymétrie peut se rencontrer dans certains contrats proposés par une plateforme en ligne : ainsi des sites de réservation d'hôtels ou de sièges de transport aérien, pour lesquels il ne fait pas de doute que l'une des parties est un professionnel. C'est encore le cas lorsque les intermédiaires ont ouvert un marché des micro-professionnels : Uber en constitue un exemple²⁸⁷.

En revanche, lorsqu'un particulier prétend fournir un service comme simple amateur, il n'obéit plus à la définition du professionnel telle qu'elle est posée par le Code de la consommation²⁸⁸. Il est vrai que certains prétendus dilettantes présentent, à y regarder de plus près, les marques du professionnalisme que sont le caractère habituel de l'activité et la recherche d'un profit substantiel²⁸⁹. Ceux-ci revêtent le masque du profane aux seules fins d'échapper à certaines obligations sociales et fiscales, ce qui leur procure d'ailleurs un avantage concurrentiel injuste²⁹⁰. La relation contractuelle entre prétendus égaux pourrait alors, théoriquement, faire l'objet d'une requalification et tomber sous l'empire du Code de la consommation. Mais encore faudra-t-il que le client ait conscience qu'il traite avec un amateur factice. Il n'en aura pas souvent les moyens.

Surtout, de nombreux contrats mettront bel et bien aux prises deux amateurs, l'un comme client, l'autre comme fournisseur d'un repas, d'un bien d'occasion ou de petits travaux. Il peut même arriver que deux particuliers se rendent des services croisés : lors d'une opération de prêt participatif, celui qui prête comme celui qui emprunte traitent habituellement avec une banque.

286. - J. Calais-Auloy et H. Temple, *Droit de la consommation*, Dalloz, 8e éd., 2010, n° 1.

287. - Le service UberPop permettait à des particuliers de se livrer au transport occasionnel de passagers à des fins lucratives, mais la loi a interdit ce service, sans porter atteinte au bloc de constitutionnalité : Conseil constitutionnel, décision n° 2015-484 QPC du 22 septembre 2015.

288. - Article préliminaire du Code de la consommation : « (...) professionnel : toute personne physique ou morale, publique ou privée, qui agit à des fins entrant dans le cadre de son activité commerciale, industrielle, artisanale, libérale ou agricole, y compris lorsqu'elle agit au nom ou pour le compte d'un autre professionnel ».

289. - S. Bernheim-Desvaux, « Le consommateur collaboratif », *Cahiers de droit de l'entreprise*, n° 3, mai 2017, dossier 15.

290. - M. Bouvard et al., *Sur l'économie collaborative : propositions pour une fiscalité simple, juste et efficace*, Rapport d'information du Sénat n° 690 fait au nom de la commission des finances, 17 septembre 2015.

Le droit civil n'est certes pas dénué de toute protection contre les injustices contractuelles. Mais certains mécanismes consuméristes n'y ont clairement pas d'équivalents : ainsi du droit de rétractation en matière de contrats conclus à distance²⁹¹.

Les relations entre particuliers bénéficient-elles d'une protection contre les clauses abusives du contrat ? Jusqu'à une époque récente, ce dispositif relevait du droit de la consommation. La réforme du 10 février 2016 semble au premier abord particulièrement opportune, qui a basculé ce mécanisme au sein du Code civil : « Dans un contrat d'adhésion, toute clause qui crée un déséquilibre significatif entre les droits et obligations des parties au contrat est réputée non écrite »²⁹². Mais le contrat d'adhésion, centre de gravité du nouveau texte, est défini comme « celui dont les conditions générales, soustraites à la négociation, sont déterminées à l'avance **par l'une des parties** »²⁹³. Or, il est tout à fait possible en pratique que le contrat intermédié ait fait l'objet d'une rédaction préalable par la plateforme, qui n'est pas partie à la convention²⁹⁴. De fait, il n'y a quasiment aucune chance que les parties veuillent et même puissent renégocier le modèle proposé par l'intermédiaire, à supposer même que l'interface du service le permette. Il ne s'agit pas d'un contrat d'adhésion au sens du Code civil, alors même qu'il en présente tous les dangers : sans doute faudra-t-il faire évoluer le texte sur ce point.

Sans aucun souci d'exhaustivité, nous envisagerons les conséquences de l'éviction du droit de la consommation au profit du droit civil relativement à deux problèmes dont l'importance pratique est remarquable : comment le discours des fournisseurs amateurs sera-t-il encadré (1) ? Quel sera l'impact de leur faible surface financière (2) ?

1 – Le discours des fournisseurs

333. **La malhonnêteté** – Lorsqu'un professionnel cherche à séduire une clientèle de consommateurs, il peut être tenté de présenter son commerce sous un jour exagérément flatteur, ou d'exercer des pressions malsaines sur le consentement d'autrui. Le droit de la consommation prévient semblables comportements en prévoyant un bouquet d'incriminations pénales dénommées « pratiques commerciales déloyales », qui se divisent en pratiques commerciales « trompeuses » et

291. - Article L. 221-18 du Code de la consommation.

292. - Article 1171 alinéa 1 du Code civil.

293. - Article 1110 alinéa 2 du Code civil.

294. - V. par ex. <https://www.taskrabbit.com/become-a-tasker> : client et fournisseur se rattachent à une catégorie de tâche à accomplir au sein de celles proposées par la plateforme TaskRabbit. Ils n'ont apparemment que quelques paramètres très simples à définir avant de passer au stade de l'exécution du contrat, sans doute parce qu'ils acceptent sans même en avoir conscience un modèle rédigé par la plateforme.

« agressives »²⁹⁵. À titre d'exemple, constitue une pratique commerciale trompeuse celle qui repose sur « des allégations, indications ou présentations fausses » portant sur « les caractéristiques essentielles du bien ou du service [...] », « le prix ou le mode de calcul du prix [...] », « l'identité, les qualités, les aptitudes et les droits du professionnel »²⁹⁶.

Dans des rapports entre particuliers, de tels mensonges seraient certes constitutifs de dol – délit civil justifiant la nullité du contrat et le versement de dommages et intérêts. Sur le plan pénal, en revanche, il faudrait s'en remettre à des infractions de droit commun telles que l'escroquerie ou l'abus de confiance, qui semblent plus difficiles à caractériser que les pratiques commerciales trompeuses.

On peut se demander s'il est justifié de traiter moins sévèrement un fournisseur qui ment ouvertement au public en s'affichant sur une plateforme, sous prétexte qu'il prodigue des services à la personne « de l'économie collaborative » à titre seulement occasionnel. Alors même que la transaction prendrait place entre « particuliers », il existe par hypothèse une asymétrie d'information, puisque l'une des parties ment en pleine conscience – la pratique commerciale trompeuse requiert une intention. Le trouble social peut être relativement important, puisque l'intermédiaire numérique est susceptible d'offrir à l'offre de contracter un très vaste rayonnement. Suivant une logique similaire à celle rencontrée précédemment en droit du travail se pose la question d'un déplacement des critères de la loi. Il prendrait ici la forme d'un éventuel décloisonnement de règles du droit de la consommation, qui pourraient par exemple s'appliquer aux propositions publiques de biens ou services, même formulées à titre occasionnel.

334. L'incompétence – Si le droit de la consommation prohibe le mensonge aux professionnels, il leur interdit également le silence en certaines occasions. Ils sont en effet débiteur d'obligations d'informations spécifiques²⁹⁷. Cette fois-ci, il est tout à fait logique qu'ils soient traités plus durement que des amateurs : la différence de compétence avec leur client étant plus importante, elle leur commande un accompagnement plus rigoureux, propre à réduire l'asymétrie.

Le droit commun des contrats prévoit certes que : « Celle des parties qui connaît une information dont l'importance est déterminante pour le consentement de l'autre doit l'en informer dès lors que, légitimement, cette dernière ignore cette information ou fait confiance à son cocontractant »²⁹⁸. Mais, dans une relation civile, la plus grande maîtrise de l'une des parties par rapport à l'autre n'est

295. - Art. L. 121-1 s. C. conso.

296. - Art. L. 121-2 C. conso.

297. - V. not. « l'obligation générale d'information précontractuelle » des art. L. 111-1 s. C. conso.

298. - Art. 1112-1 al. 1. du Code civil.

qu'envisagée comme une possibilité, alors qu'elle était postulée comme une certitude dans la matière consumériste. La conséquence est claire : l'amateur véritablement peu compétent n'a pas à dispenser information et conseils à son client également ignorant, car il n'est pas en mesure de le faire. Le résultat peut être redoutable. Nous avons vu que les plateformes constituent des courtiers d'un nouveau genre, qui se contenteront la plupart du temps de prodiguer aux parties des conseils standardisés et superficiels²⁹⁹. Dès lors, il n'y aura plus personne pour délivrer un accompagnement fiable et personnalisé au client traitant avec un dilettante. L'un d'eux pourra se lancer dans une opération de prêt participatif vouée à l'échec sans être en mesure d'en prendre conscience à temps³⁰⁰. Un autre fera appel à un bricoleur du dimanche mettant en œuvre des techniques ou des matériaux parfaitement inadaptés à sa situation.

Admettons qu'on ne peut pas, en général, attendre des dilettantes qu'ils se soumettent à un devoir de conseil substantiel. Leur responsabilité civile sera tout de même susceptible d'être engagée sur d'autres fondements. Surgira alors éventuellement une autre difficulté, tenant à leur faible surface financière.

2 – La surface financière des fournisseurs

335. Le recours aux assurances – Qu'il ait commis un dol dans la formation du contrat, ou qu'il ait échoué à accomplir une prestation promise, ou encore qu'il ait causé des dégâts aux biens ou aux personnes dans l'accomplissement de la tâche qui lui était confiée, l'amateur est susceptible d'engager sa responsabilité civile. Dans certains cas, une assurance aura obligatoirement été souscrite – par exemple, en cas de conduite d'un véhicule terrestre à moteur. Lorsque tel n'est pas le cas, ou lorsque les dommages causés n'entrent pas dans les limites de la couverture, le dilettante devra répondre des indemnités sur son patrimoine personnel. Il peut se révéler insuffisant, en particulier en cas de dommage corporel. Une telle situation ne se produit que rarement face à un professionnel : l'exercice plus régulier d'une activité dangereuse pour les tiers crée les conditions et les incitations nécessaires à la souscription volontaire d'une assurance, quand bien même la loi ne le commanderait pas.

Nous savons qu'en principe, la plateforme n'est pas responsable de la bonne fin du contrat dont elle a favorisé la conclusion par son entremise. Mais si les intermédiaires ne sont pas automatiquement débiteurs d'une telle obligation, ils peuvent en être chargés par le contrat ou par la

299. - V.supra, n°322.

300. - La proposition peut désigner aussi bien le prêteur que l'emprunteur.

loi : c'est le mécanisme du *ducroire*³⁰¹. Il est donc loisible au législateur d'obliger certaines plateformes à se mêler de l'exécution du contrat de base³⁰². Dans ce cas, il est évident qu'elles s'assureraient contre les risques patrimoniaux nés de cette obligation, et qu'elles rémunéreraient cette couverture par un prélèvement sur leurs bénéfices.

C'est une voie un peu différente qui semble suivie par la pratique. Plusieurs plateformes, en effet, ont d'ores et déjà choisi de faciliter l'indemnisation des dommages causés par les contrats qu'elles suscitent, en souscrivant des produits assurantiels. Dans ces exemples, la voie choisie est celle de l'assurance pour compte³⁰³. La plateforme intervient comme simple souscripteur et, à ce titre, contracte et rémunère la couverture. C'est le client qui endosse les qualités d'assuré — celui dont la personne ou le patrimoine est exposé au risque — et de bénéficiaire — celui qui profitera de la prestation en cas de sinistre.

À titre d'exemple, la société Blablacar a souscrit une assurance pour compte procurant aux passagers en covoiturage des garanties supplémentaires par rapport à celles qui résultent de la simple souscription d'une assurance obligatoire couvrant les dommages aux tiers³⁰⁴. AirBnB offre de la même manière une protection à « ses hôtes » contre les dégâts causés par les personnes hébergées³⁰⁵. TaskRabbit a prévu une couverture d'un maximum d'un million de dollars « (...) *for Losses arising from Property Damage as a direct result of Negligence of a Tasker during performance of a Task* »³⁰⁶.

L'assureur *solvens* peut ensuite se retourner contre le responsable, si celui-ci se trouve dans une situation où il engage sa responsabilité civile.

301. - A propos du *ducroire* contractuel en matière de courtage : N. Dissaux, V° « Courtage », art. préc. n° 146 s. Pour un cas de *ducroire* légal, applicable à cet intermédiaire qu'est le commissionnaire de transport, V. l'art. L. 132-4 du Code des transports.

302. - Si la plateforme est un « faux courtier » qui prend fermement la direction du marché sous-jacent, la voie de la responsabilité délictuelle du commettant du fait de ses préposés pourrait être explorée pour l'atteindre.

303. - Art. L. 112-1 al. 2 du Code des assurances : « L'assurance peut aussi être contractée pour le compte de qui il appartiendra. La clause vaut, tant comme assurance au profit du souscripteur du contrat que comme stipulation pour autrui au profit du bénéficiaire connu ou éventuel de ladite clause ».

304. - <https://www.blablacar.fr/assurance-covoiturage>. La page précise bien que l'assurance automobile obligatoire couvre les dommages aux tiers, et présente les garanties additionnelles. On lit notamment que « En cas d'immobilisation du véhicule lors d'un trajet avec réservation en ligne, le remorquage et l'acheminement du conducteur et des passagers à destination sont pris en charge si vous n'êtes pas déjà couvert ». Le contrat passé avec l'assureur Axa est consultable à l'adresse https://www.blablacar.fr/images/insurance/Notice_d_informat_on_BLABLACAR_FR.pdf.

305. - <https://www.airbnb.fr/host-protection-insurance>. Cela démontre d'ailleurs que la victime du dommage peut être le fournisseur du service et non seulement celui qui en bénéficie contre rémunération.

306. - <https://www.taskrabbit.com/pledge>.

Sur un plan purement économique, la différence n'est sans doute pas très grande avec la situation dans laquelle la plateforme procéderait elle-même à l'indemnisation, puis appellerait son assureur en garantie. En revanche, sur le plan symbolique, le mécanisme choisi est particulièrement habile puisqu'il préserve l'image d'un intermédiaire extérieur à la relation de base, et contre lequel aucun recours ne peut être dirigé, tout en donnant l'impression « d'offrir » gracieusement un service à ses utilisateurs. Ici aussi, relevons qu'une assurance pour compte pourrait être imposée par la loi, au besoin, si des plateformes manquaient de souscrire volontairement des couvertures pour autrui dans des secteurs où leurs armées d'amateurs sont source de dommages.

LE CONTRAT : CONCLUSION

L'ère numérique est celle de l'information abondante et peu chère. À ce titre, elle pouvait susciter l'espoir d'un monde contractuel meilleur, dans lequel des parties bien renseignées, souples et agiles, passent en un instant des conventions toujours conformes à leur parfait intérêt. Mais le progrès ne toucherait pas seulement les manières de contracter. Des bataillons de petits professionnels et d'amateurs, jusqu'ici relégués dans l'ombre, seraient tout à coup propulsés sous les puissants projecteurs des plateformes. Un pan nouveau de la vie économique accèderait à l'existence, dans lequel la course à la concentration du capital n'apparaîtrait plus nécessaire pour constituer un partenaire contractuel visible. Cette économie « collaborative » révélerait le talent caché du voisin, mobiliserait les richesses dormant dans les greniers et les garages, et assurerait la promotion, sur le marché, de valeurs auparavant secondaires : le partage, la solidarité, la sensibilité à l'environnement.

Sans nier la réalité des progrès que l'on doit à la numérisation des contrats, il s'est agi de peindre de ces différentes évolutions un tableau plus nuancé, en révélant la part de menaces qu'elles recèlent.

L'étude a débuté par les mouvements communs à tous les contrats.

Au stade de la formation, il est apparu que les parties recherchaient avant tout la rapidité et la simplicité du processus. Si l'on peut douter que les contrats hors-ligne soient lus, on peut être certain que les contrats électroniques ne le sont pas, alors même qu'ils présentent des dangers qui leur sont propres. Des modèles d'affaires spécifiques à Internet y pullulent, reposant sur l'échange d'un service contre des données personnelles, sur des gratuités temporaires ou partielles. Il n'est pas certain que le public en saisit toujours la portée véritable avant de s'engager. Le danger est aggravé par la prolifération de conditions générales qui trahissent l'origine américaine des géants du

secteur : il s'agit parfois de traductions serviles des *terms of service*, parfaitement inadaptées aux droits français et européen, remplies de clauses abusives propres à tromper les usagers sur l'étendue de leurs devoirs et de leurs prérogatives. Toujours pour favoriser un accord des volontés simple et rapide, le commerce électronique se contente de procédés d'identification très faibles, qui font surgir de graves questions sur les plans de la preuve et de l'imputabilité du contrat. Les procédés de signature électronique restent largement inutilisés, à la fois parce que leur complexité risquerait de ralentir les élans consuméristes du public, et parce que les pouvoirs publics n'ont pas encore assumé leur éventuelle fonction de garant des identités en ligne.

Au stade de l'exécution des conventions, l'étude s'est faite plus prospective. Les *smart contracts*, qui pourraient occuper une place importante dans la pratique des prochaines décennies, n'en sont qu'à leurs balbutiements. Ils reposent sur une chaîne de blocs (*blockchain*) — un registre chiffré et distribué de transactions —, doublée d'une couche logicielle spécifique, qui se comportera comme un huissier numérique impitoyable. Dès lors que certaines conditions seront réunies, elle procèdera à des mesures d'exécution, en procédant à des mouvements de monnaie, ou en adressant des instructions à des objets connectés. La technique est de nature à diminuer les coûts de transaction dans certains secteurs, ouvrant par exemple de nouveaux marchés aux assureurs en matière de micro-risques. Toutefois, il est important de souligner que la sentinelle logicielle n'obéit ni à un contrat, ni au droit en général, mais à des lignes de code. Celles-ci peuvent mimer dans une certaine mesure le fonctionnement du système juridique, mais n'y parviendront jamais parfaitement, et peuvent même être conçues en l'ignorant superbement. Les *smart contracts* rejoignent ainsi les mesures techniques de protection au sein des illustrations les plus marquantes de la concurrence qui oppose norme juridique et norme informatique.

L'étude s'est poursuivie par les transformations affectant certains contrats spéciaux, à l'occasion de la montée en puissance de l'économie de plateformes.

Auparavant, les géants du capitalisme étaient des acteurs de marché : ils prenaient une part active et personnelle à la fourniture de biens et de services. Les intermédiaires n'occupaient alors qu'une place de second rang ; les voici devenus princes. Plaçant face à face des myriades de petits fournisseurs et de petits clients, ils tiennent leur sort à la merci de leurs algorithmes de classements, et prélèvent une part de la valeur ajoutée qui va croissant. Juridiquement, leur position est confortable : courtiers d'un nouveau genre, ils flottent au-dessus du marché et n'assument pas les mêmes obligations que ceux qui y prennent pied. Même si on les compare aux intermédiaires traditionnels, ils paraissent en retrait : le devoir de conseil personnalisé et rigoureux attendu par

exemple d'un courtier en assurances est incompatible avec leur modèle économique, qui repose sur des coûts de transaction tendant vers zéro. Le conseil est algorithmique et standardisé.

À cette montée en puissance des contrats d'intermédiaire correspond une déstabilisation des contrats applicables aux parties intermédiées. Les fournisseurs sont ainsi considérés comme des professionnels indépendants, par conséquent inéligibles aux protections traditionnellement attachées au contrat de travail. Pourtant, certaines plateformes semblent outrepasser leur fonction d'entremise pour prendre discrètement la direction du marché sous-jacent : à ce titre, elles méritent parfois d'être qualifiées d'employeuses. Mais lorsque ce n'est pas possible, la question se pose du basculement de certaines protections sociales liées au salariat vers un ensemble plus vaste, comprenant l'activité indépendante. Le législateur a récemment amorcé un mouvement dans cette direction. Du point de vue des clients, c'est un autre droit contractuel asymétrique qui se trouve parfois évincé : celui de la consommation. Lorsqu'il a recours aux biens et services proposés par des amateurs, le client se trouve théoriquement dans une relation entre égaux qui le prive des bienfaits auxquels l'avait habitué la législation consumériste. La question d'un meilleur encadrement du discours des fournisseurs amateurs a été posée. Celle de leur faible surface financière semble en voie d'être résolue par le recours à des contrats d'assurance pour compte, rémunérés par la plateforme et couvrant les dommages éventuels aux clients, recours qui pourrait être systématisé.

Bibliographie

I – Ouvrages généraux

- C. Atias, *Droit civil. Les biens*, Lexisnexus, 12e éd., 2014.
- B. Beigner, B. de Lamy et E. Dreyer (ss. la dir.), *Traité de droit de la presse et des médias*, Litec, 2009.
- H. Bitan, *Droit et expertise du numérique. Créations immatérielles, données personnelles, e-réputation, droit à l'oubli, neutralité, responsabilités civile et pénale*, Lamy, coll. Axe droit, 2015.
- P. Breton, *Une histoire de l'informatique*, éd la Découverte, 1987.
- J.-M. Bruguière et B. Gleize, *Droits de la personnalité*, éd. Ellipses, 2015.
- J. Calais-Auloy et H. Temple, *Droit de la consommation*, Dalloz, 8e éd., 2010.
- C. Caron, *Droit d'auteur et droits voisins*, Litec, 4e éd., 2015.
- C. Castets-Renard, *Droit de l'internet. Droit français et européen*, Montchrestien-Lextenso, 2e éd., 2012.
- G. Cornu (dir.), *Vocabulaire juridique de l'Association Henri Capitant*, 11e éd., 2016.
- W. Dross, *Droit des biens*, LGDJ, 2e éd., 2014.
- C. Féral-Schuhl, *Cyberdroit. Le droit à l'épreuve de l'internet*, Dalloz, 6e éd., 2010.
- P. Gaudrat et F. Sardain, *Traité de droit civil du numérique, t. 1, Droit des biens*, Larcier, 2015.
- P. Gaudrat et F. Sardain, *Traité de droit civil du numérique, t. 2, Droit des obligations*, Larcier, 2015.
- G. Goubeaux, *Traité de droit civil. Les personnes*, LGDJ, 1989, dir. J. Ghestin.
- G. Gromov, *Roads and crossroads of the Internet history* : http://www.netvalley.com/internet/history_of_internet.pdf.
- L. Grynbaum, C. Le Goffic et L. Morlet-Haïdara, *Droit des activités numériques*, Dalloz, 2014.
- A. Hollande et X. Linant de Bellefonds, *Pratique du droit de l'informatique et de l'internet*, Editions Delmas, 6e éd., 2008.
- E. C. Lallana et M. N. Uy, *The information age*, UNDP-APDID, 2003.
- E. Lazard et P. Mounier-Kuhn, *Histoire illustrée de l'informatique*, EDP sciences, 2016.
- P. Malaurie et L. Aynès, *Les biens*, Defrénois, 5e éd., 2013.
- P. Malaurie, L. Aynès et P. Stoffel-Munck, *Droit des obligations*, LGDJ, 8e éd., 2016.

P. Malinvaud, *Introduction à l'étude du droit*, Lexisnexis, 14e éd., 2013.

M. Planiol, *Traité élémentaire de droit civil conforme au programme officiel des facultés de droit. Tome 1, Principes généraux, les personnes, la famille, les incapables, les biens*, LGDJ, 5e éd., 1908.

J. Ryan, *A history of the internet and the digital future*, Reaktion books, 2010.

F. Terré, *Introduction générale au droit*, Dalloz, 9e éd., 2012.

F. Terré et D. Fenouillet, *Droit civil. Les personnes. Personnalité, incapacité, protection*, Dalloz, 8e éd., 2012.

F. Terré et P. Simler, *Droit civil. Les biens*, Dalloz, 9e éd., 2014, n° 79.

F. Terré, P. Simler et Y. Lequette, *Droit des obligations*, Dalloz, 10e éd., 2009.

M. Vivant et J.-M. Bruguière, *Droit d'auteur et droits voisins*, Dalloz, précis, 3e éd., 2016.

M. Vivant (ss. la dir.), *Lamy droit du numérique*, 2017.

II - Ouvrages spéciaux, thèses, monographies

P. Baran, *Research memorandum on a distributed command and control system configuration*, RM-2632, 31 décembre 1960 :

http://www.rand.org/content/dam/rand/pubs/research_memoranda/2009/RM2632.pdf.

B. Beignier, *L'honneur et le droit*, LGDJ-Lextenso, 2015.

T. Berners-Lee, *Weaving the web : the original design and ultimate destiny of the World wide web by its inventor*, Harper San Francisco, 2000.

V.-L. Bénabou et J. Rochfeld, *À qui profite le clic ?*, éd. O. Jacob, 2015.

J. Carbonnier, *Flexible droit, pour une sociologie du droit sans rigueur*, LGDJ, 10e édition, 2001.

D. Cardon, *À quoi rêvent les algorithmes ? Nos vies à l'heure des big data*, Seuil, 2015.

A. Casilli et D. Cardon, *Qu'est-ce que le digital labor ?*, INA, 2015.

P. Catala, *Le droit à l'épreuve du numérique. Jus ex machina*, PUF, 1998.

J. Cattani, *Le droit de l'accès aux communications électroniques*, préf. R. Mehdi et H. Isar, PUAM, 2015.

A. Chaigneau, (dir.), *Fonctions de la propriété et communs. Regards comparatistes*, Société de législation comparée, vol. 27, 2017.

M. Clément-Fontaine, *L'œuvre libre*, préf. M. Vivant, éd. Larcier, 2014.

B. Coriat (dir.), *Le retour des communs : la crise de l'idéologie propriétaire*, Les liens qui libèrent, 2015.

A. Debet, J. Massot et N. Metallinos (ss. la dir.), *Informatique et libertés. La protection des données à caractère personnel en droit français et européen*, Lextenso, 2015.

L. Duguit, *Les transformations générales du droit privé depuis le Code Napoléon*, éd. F. Alcan, 2e

éd., 1920.

S. Dusollier, *Droit d'auteur et protection des œuvres dans l'univers numérique*, Larcier, 2005.

J. Eynard, *Les données personnelles. Quelle définition pour un régime de protection efficace ?*, éd. Michalon, 2013.

A. Garapon et J. Lassègue, *Justice digitale*, PUF, hors collection, 2018.

J.-G. Ganascia, *Le mythe de la singularité : faut-il craindre l'intelligence artificielle ?*, éd. Du Seuil, 2017.

D. Gutmann, *Le sentiment d'identité. Etude de droit des personnes et de la famille*, LGDJ, 2000.

A. Hodges, *Alan Turing ou l'énigme de l'intelligence*, trad. N. Zimmermann, Payot, 1988.

L. Josserand, *De l'esprit des droits et de leur relativité : théorie dite de l'abus des droits*, Dalloz, 1939.

H. Le Crosnier, *En communs : une introduction aux communs de la connaissance*, C&F éditions, 2015.

P. Léger, *La recherche d'un statut de l'oeuvre transformatrice. Contribution à l'étude de l'oeuvre composite en droit d'auteur*, dir P. Sirinelli, 2015.

L. Lessig, *Free Culture*, The Penguin Press, 2004.

L. Lessig, *L'avenir des idées*, trad. française J.-B. Soufron et A. Bony, préf. J.-C. Guédon, Presses Universitaires de Lyon, 2005.

L. Lessig, *Code 2.0*, Basic Books, 2006.

E. Liberge et A. Delalande, *Le cas Alan Turing. Histoire extraordinaire et tragique d'un génie*, Les arènes BD, 2015.

J.-F. Mouhot, *Des esclaves énergétiques*, éd. Champ Vallon, 2011.

E. Ostrom, *Gouvernance des biens communs : pour une nouvelle approche des ressources naturelles*, trad. L. Baechler, De Boeck, 2010.

E. Pariser, *The filter bubble : how the new personalized web is changing what we read and how we think*, Penguin books, 2012.

J. Rifkin, *The Age of Access : The New Culture of Hypercapitalism, Where All of Life Is a Paid-For Experience*, New York, Jeremy P. Tarcher/Putnam, 2000.

J. Rifkin, *La troisième révolution industrielle*, Actes sud, 2013.

J. Rochfeld, *Les grandes notions du droit privé*, PUF, 2013, 2e éd.

E. Sadin, *La silicolonisation du monde. L'irrésistible expansion du libéralisme numérique*, éd. L'échappée, 2016.

B. van Schewick, *Network neutrality and quality of service. What a non-discrimination rule should look like*, The Center for Internet and Society, 11 juin 2012.

R. Stamboliyska, *La face cachée d'Internet*, Larousse 2017.

III - Articles, fascicules

H. Allcott et M. Gentzkow, « Social media and fake news in the 2016 election », *Journal of Economic Perspectives*, Volume 31, Number 2, Spring 2017, p. 211.

P. Aigrain, « Comment délimiter le partage non-marchand entre individus ? », note du blog paigrain.debatpublic.net du 13 février 2012.

P. Aigrin, « Culture et partage : les conditions d'existence des communs culturels », note du blog paigrain.debatpublic.net, du 9 décembre 2012.

George A. Akerlof, « The Market for "Lemons": Quality Uncertainty and the Market Mechanism », *The Quarterly Journal of Economics*, Vol. 84, No. 3. (Aug., 1970), p. 488.

N. Anderson, « Deep packet inspection meets 'Net neutrality, CALEA », article arsetechnica.com du 26 juillet 2007.

J. Antippas, « Propos dissidents sur les droits dits “patrimoniaux” de la personnalité », *RTD. com.*, 2012, p. 35.

W. Audureau et S. Seelow, « Comment fonctionnent les blocages de sites djihadistes », article lemonde.fr du 17 mars 2015.

D. Aurebach, « Internet n'a pas résolu par magie les imperfections des marchés », article slate.fr du 15 juin 2015.

A. Ayewouadan « La preuve des actes juridiques sous le prisme des contrats électroniques », *RLDI*, 2009, n° 45, p. 73, spéc. n° 31.

T. Azzi, « Open data et propriété intellectuelle. État des lieux au lendemain de l'adoption de la loi pour une République numérique », *D.*, 2017, p. 583.

J. Ball, « Meet the seven people who hold the keys to the worldwide internet security », article theguardian.com du 28 février 2014.

L. Ballet, « Text & Data Mining, l'impossible exception », *Dalloz IP/T*, 2016, p. 415.

K. Banner et W. Sui-Lee, « Apple removes New York Times apps from its store in China », article nytimes.com du 4 janvier 2017.

C. Béguin-Faynel, « Pour un testament des dernières volontés numériques », in *Traité des nouveaux droits de la mort. La Mort, incarnation(s) cadavérique(s)*, dir. M. Touzeil-Divina, M. Bouteille-Brigant et J.-F. Boudet, éd. L'Épilogue, 2014, chap V, section 3.

V.-L. Bénabou et J. Rochfeld, « Les moteurs de recherche, maîtres ou esclaves du droit à l'oubli numérique ? Acte I : Le moteur, facilitateur d'accès, agrégateur d'informations et responsable de traitement autonome », *D.*, 2014, p. 1476.

V.-L. Bénabou, « Entrée par effraction d'une notion juridique nouvelle et polymorphe : le contenu numérique », *Dalloz IP/IT*, 2017 p. 7.

P.-J. Benghozi, « Blockchain : objet à réguler ou outil pour réguler ? », *JCP E*, 2017, n° 36, 1470.

Y. Benkler, « From Consumers to Users: Shifting the Deeper Structures of Regulation Toward Sustainable Commons and User Access », *Federal Communications Law Journal*, 200, vol. 52: Iss. 3, Article 9

- A. Bensamoun, « Des robots et du droit... », *Dalloz IP/IT*, 2016, 281.
- A. Bensamoun et J. Groffe, « Création numérique », in *Rép. civ. Dalloz*, juin 2014, n° 166.
- A. Bensoussan, « Droit des robots : science-fiction ou anticipation ? », *D.*, 2015, p. 1640.
- S. Bernheim-Desvaux, « Le consommateur collaboratif », *Cahiers de droit de l'entreprise*, n° 3, mai 2017, dossier 15.
- C. Berrebi et S. Vatin, « Le crowdfunding en pratique, opportunités et limites », *JCP G*, 2014 n° 49, 1266.
- C. Berthet, « Chiffrement et lutte contre le terrorisme : attention à ne pas se tromper de cible », tribune publiée sur *lemonde.fr* le 22/08/16.
- C. Berthet, C. Zolynski, N. Anciaux et P. Pucheral, « Contenus numériques, récupération des données et empouvoirement du consommateur », *Dalloz IP/IT*, 2017, p. 29.
- T. Berthier, « La robotique et le temps du Kronos », article *humanoides.fr* du 29 juin 2016.
- I. Beyneix, « Le traitement des données personnelles par les entreprises : big data et vie privée, état des lieux », *JCP G*, 9 nov. 2015, n° 46-47, doct. 1260
- A. Blake, « Kellyanne Conway says Donald Trump's team has "alternative facts"... », article *thewashingtonpost.com* du 22 janvier 2017.
- R. Bonhomme, V° « Virement », in *Rép. com. Dalloz*, octobre 2014.
- T. Bonneau, « Le financement participatif . - Ord. 30 mai 2014, D. 16 sept. 214 et AA. 22 et 30 sept. 2014 », *JCP E*, n° 42, 16 oct. 2014, 1523.
- J. Bossan, « Le droit pénal confronté à la diversité des intermédiaires de l'Internet », *RSC*, 2013, 295.
- C. Bourdoiseau, « Generali veut réinventer l'assurance avec "Vitality" », article *argusdelassurance.com* du 24/06/16.
- D. Bourg et al., « "La Troisième Révolution" de Rifkin n'aura pas lieu », article *liberation.fr* du 21 octobre 2014.
- C. Bondard, et al., « Blockchain – Quelques utilisations actuelles de cet outil en droit des affaires. Monnaies virtuelles, transmission des instruments de paiement, outils de financement, smart contracts, etc. », *JCP E*, 2017, n° 36, 1471.
- R. Botsman, « The sharing economy lacks a shared definition », article *fastcompany.com* du 21 novembre 2013.
- X. Boy, « Conv. EDH, art. 10 : liberté d'expression et de la presse » in *Répertoire Dalloz de droit européen*.
- L. Breuker, « Le support de création et le support de commercialisation de l'œuvre », *CCE*, n° 1, janv. 2003, chron. 2.
- B. Britto, « Animatronic pets at retirement homes a sign of how robots will contribute to our lives », article *baltimoresun.com* du 30 mars 2017.
- S. Broca et P. Eynaud, « Biens communs et outils numériques : le cas des logiciels libres », *Juris associations*, 2014, n° 501, p. 33.

- J.-M. Bruguière, « Droit à l'oubli numérique des internautes ou... responsabilité civile des moteurs de recherche du fait du référencement ? », *CCE*, mai 2015, n° 5, p. 15
- E. Brunet, « Règlement général sur la protection des données à caractère personnel. Genèse de la réforme et présentation globale », *Dalloz IP/IT*, 2016, p. 567.
- R. Cabrillac, « Opposabilité d'une clause de non-garantie dans une chaîne homogène de contrats translatifs de propriété », *D.*, 2006, 971.
- Par ex. J. Calais-Auloy, « L'influence du droit de la consommation sur le droit civil des contrats », *RTD. civ.*, 1994, p. 239.
- G. Canivet, « Blockchain et régulation », *JCP E*, 2017, n° 36, 1469.
- E. Caprioli, F. Mattatia et S. Vulliet-Tavernier, « L'identité numérique. Entretien », *Cahiers de droit de l'entreprise*, mai 2011, entretien 3.
- E. Caprioli et al., « Blockchain et smart contracts : enjeux technologiques, juridiques et business », *Cahiers de droit de l'entreprise*, n° 2, mars 2017, entretien 2.
- A. Casilli, « Contre l'hypothèse de la "fin de la vie privée" », *Revue française des sciences de l'information et de la communication*, n° 3, 2013.
- C. Castets-Renard, « Le formalisme du contrat électronique ou la confiance décrétée », *Defrénois*, 2006, n° 20, p. 1529.
- C. Castets-Renard, « Des biens aux services numériques : de l'ère de la propriété à l'âge de l'accès », in *Les biens numériques*, éd. Ceprisca, 2015, p. 203.
- D. Castro, « A declaration of the Interdependance of Cyberspace », article *computerworld.com* du 8 février 2013.
- P. Catala, « L'immatériel et la propriété », in *Le droit et l'immatériel, Archives de philosophie du droit*, t. 43, p. 63.
- N. Catelan, « La protection pénale du droit d'auteur : une négligence caractérisée ? », *RLDI*, 2001, n° 67.
- J. Cattan, « La protection de la neutralité de l'internet : pour un accès neutre aux biens numériques » in *Les biens numériques*, éd. Ceprisca, 2015, p. 43.
- H. Causse, « Le contrat électronique, technique du commerce électronique », in *Le contrat électronique. Au cœur du commerce électronique, journées d'études organisées par le DJCE de Poitiers*, LGDJ, 2005, p. 11.
- V. Cerf et B. Aboba, « How the internet came to be », article *netvalley.com*, 1993.
- A. Chaigneau, « Propriété et souveraineté de l'Internet : la maîtrise d'une infrastructure », in *Les biens numériques*, éd. Ceprisca, 2015, p. 18.
- G. Champeau, « Bruxelles veut interdire le blocage de la VoIP sur les mobiles », article *numerama.com* du 7 décembre 2009.
- G. Champeau, « Sosh lance un forfait avec Facebook et Twitter illimités, sans internet », article *numerama.com* du 6 février 2012.
- L. Chapin et C. Owens, « Interconnection and peering among internet service providers. A historial perspective. An interisle white paper », 2005, article *interisle.net*.

- G. Chantepie, « l'exigence de clarté dans la rédaction du contrat », *Revue des contrats*, n° 2012/3, p. 989.
- Y. Charpenel, « Le Darkweb, un objet juridique parfaitement identifié. Le paradis, l'enfer ? », *Dalloz IP/IT*, p. 71.
- V. Charpiat, « Le bitcoin devient monnaie courante : les monnaies digitales entre transparence et innovation », *Revue des Juristes de Sciences Po*, n° 9, juin 2014.
- S. Chassagnard-Pinet, « A la recherche d'une définition de "l'économie collaborative" », *Cahiers de droit de l'entreprise*, mai 2017, n° 3, article 11.
- J.-P. Chauchard, « Les avatars du travail indépendant », *Droit social*, 2009, p. 1065.
- L. Chemla, « Nous sommes tous des ayants droit », article *liberations.fr/ecrans/* du 23/10/13.
- O. Chicheportiche, « Censure sur l'AppStore : Apple s'emmêle les pinceaux avec un Prix Pulitzer », article *zdnnet.fr* du 19 avril 2010.
- F. Chopin, « Téléchargement illégal et Hadopi », *AJ pénal*, 2012, 528.
- F. Chopin, « Cybercriminalité » in *Rép. pén. Dalloz*, avril 2017.
- G. Clamour, « La signature électronique dans les marchés publics », *Contrats et marchés publics*, 2012, n° 8, p. 25.
- M. Clément-Fontaine, « L'œuvre libre », fasc. 1975 in *J.-Cl. Propriété littéraire et artistique*, 22 juillet 2014.
- M. Clément-Fontaine, « La clause non commerciale des licences ouvertes : sécurité juridique, libre concurrence et valorisation », *AJCA*, 2015, p. 164.
- M. Clément-Fontaine, « L'œuvre numérique : un élément iconoclaste en droit de la propriété » in *Les biens numériques*, éd. Ceprisca, 2015, p. 183.
- M. Clément-Fontaine, « La genèse de l'économie collaborative : le concept de communauté », *Dalloz IP/IT*, 2017, 140.
- Y. Cohen-Adria, « Blockchain : révolution ou évolution ? », *Dalloz IP/IT*, 2016, p. 537.
- P.-H. Conac, « Le nouveau régime du financement participatif », *Rev. sociétés*, 2014, p. 461.
- S. Crocker, « Request for comments 1. Host software » : <http://tools.ietf.org/html/rfc1>.
- M. Dalle, « Réflexions sur l'éducation des internautes au respect du droit d'auteur », in *Les biens numériques*, éd. Ceprisca, 2015, p. 89.
- G. DangNguyen, S. Dejean et T. Pénard, « Gratuité sur Internet : entre logiques individuelles et logiques communautaires », in *La gratuité. Un concept aux frontières de l'économie et du droit*, LGDJ, 2013, p. 91.
- M. Daury-Fauveau, « Le "vol d'un bien numérique : vers la suppression des guillemets », in *Les biens numériques*, éd. Ceprisca, 2015, p. 137.
- M. Dary et L. Benaissa, « Privacy by design : un principe de protection séduisant, mais complexe à mettre en œuvre », *Dalloz IP/IT*, 2016, p. 476.
- N. Deffains et J.-B. Thierry, « Fausses nouvelles » in *Rép. pén. Dalloz*, juillet 2015.

- A. Delcambre, « Huit médias français s'allient à Facebook contre les "fake news" », article *lemonde.fr* du 06 février 2017.
- X. Delpech, « La délicate appréhension de la Blockchain par le droit », *AJ contrat*, 2017, p. 244.
- A. Denizot, « La loi pour une République numérique : tous législateurs ? », *RTD. civ.*, 2017, p. 232.
- J. Devèze, « Vive l'article 1322 ! Commentaire critique de l'article 1316-4 du Code civil », in *Mélanges Catala*, Litec, 2001, p. 529.
- N. Dissaux, V° « Courtage » in *Rép. commercial Dalloz*, avril 2017.
- C. Doctorow, « An open letter to the W3C Director, CEO, team and membership », article *eff.org* du 18 septembre 2017.
- B. Dondero, « Justice prédictive : la fin de l'aléa judiciaire ? », *D.*, 2017, p. 532.
- E. Dreyer, « Les nouvelles responsabilités sur Internet », *AJ pénal*, 2013, p. 15
- E. Dreyer, « Le blocage de l'accès aux sites terroristes ou pédopornographiques », *JCP G*, 6 avr. 2015, doct., 423.
- E. Dreyer, « Injures publiques et non publiques », in *Rép. pén. Dalloz*, févr. 2017.
- S. Drillon, « La révolution Blockchain », *RTD. com.*, 2016, p. 893.
- O. Dumons, « Des hôpitaux français eux aussi victimes de chantage informatique », article *lemonde.fr*, rubrique pixels, du 24/02/16.
- C. Durand, « Les données d'Uber sur la circulation, une mine d'or pour les villes et leurs urbanistes », article *Numerama.com* du 9/01/17.
- E. Dvinina, « Etats-Énis : quelle riposte aux piratages russes ? », article *lemonde.fr* du 19 décembre 2016.
- P. Eckersley, « How online tracking companies know most of what you do online (and what social networks are doing to help them) », article *eff.org* du 21/09/09.
- Y. Eudes, « Comment le FBI a fait tomber Silk Road », article *lemonde.fr* du 09/09/14.
- D. S. Evans et R. Schmalensee, « Why winner-takes-all thinking doesn't apply to the platform economy », article *Harvard Business Review*, *hbr.org*, 04/05/16.
- C. Farivar, « Axanar isn't fair use, judge finds, setting stage for Star Trek copyright trial », article *arstechnica.com* du 1er mai 2017.
- M. Ferhallad, « L'ex équipier Quick mis en examen pour diffamation », article du 11/01/14, *laprovence.com*.
- P. Filippi (de) et S. Hassa, « Blockchain technology as a regulatory technology : From code is law to law is code », article *firstmonday.org* du 5 décembre 2016.
- P. Filippi (de), « Il faut davantage enseigner la technologie aux juristes », entretien avec le cabinet Deloitte sur *equationdelaconfiance.fr*, non daté.
- P. Filippi (de), « What Blockchain means for the sharing economy », *Harvard Business Review*, 15 mars 2017.
- K. Finley, « A \$50 million hack just showed that the DAO was all too human », article *wired.com*

du 18 juin 2016.

J. Fioretti, « EU increases pressure on Facebook, Google and Twitter over user terms », article *reuters.com* du 24 juillet 2017.

J. Francillon, « Piratage numérique », *RSC*, 2006, 93.

J. Francillon, « Messages racistes ou antisémites postés sur le réseau social Twitter », *RSC*, 2013, 566.

FTC, « VIZIO to pay \$2.2 million to FTC, state of new jersey to settle charges it collected viewing histories on 11 million smart televisions without users' consent », article *ftc.gov* du 6/02/17.

A. Garapon, « Les enjeux de la justice prédictive », *JCP G*, 2017, doct. 31.

W. Gardner Selby, « Ted Cruz incorrect about Obama giving control of internet to UN-like body », article *politifact.com* du 14 septembre 2016.

S. Gavois, « Il y a 20 ans, John Barlow publiait sa déclaration d'indépendance du cyberspace », article *netxinpact.com* du 8 février 2016.

G. Gebhart et E. Harmon », FCC abandons zero-rating investigation and moves backward on net neutrality », article *eff.org* du 9 février 2017.

E. Geffray, « Quelle protection des données personnelles dans l'univers de la robotique ? », *Dalloz IP/IT*, 2016, p. 295.

D. Gibirila, V^o « Effets de commerce », in *Rép. com. Dalloz*, janvier 2010.

P. Golle, « Revisiting the uniqueness of simple demographics in the US population » : <https://crypto.stanford.edu/~pgolle/papers/census.pdf>.

J.-L. Goutal, « Logiciel : l'éternel retour », in *Droit et techniques. Etudes à la mémoire du professeur Xavier Linant de Bellefonds*, Lexisnexis, 2007, p. 217

A. Greenberg, « It's been 20 years since this man dec'ared cyberspace independence », article *wired.com* du 2 août 201

A. Grondin, « Google s'en remet aux internautes pour évacuer les "fake news" des recherches », articles *leschos.fr* du 26 avril 2017.

G. Gross, « Stanford professor files net neutrality complaint against Verizon Wireless », article *computerworld.com* du 19 décembre 2011.

L. Grynbaum, « La preuve littérale. Dispositions générales. Ecrit électronique », in *Juris-Classeur civil*, art. 1316 à 1316-4, fascicule 10, décembre 2016.

G. Guerlin, « Considérations sur les smart contracts », *Dalloz IP/IT*, octobre 2017.

N. Guibert, « La démocratie, nouvelle cible de la cyberguerre », article *lemonde.fr* du 20 février 2017.

D. Guinier, « Une signature numérique insatisfaisante est-elle encore une signature ? », *Gaz. Pal.*, 19 avr. 2001, p. 14.

D. Gutmann, « Du matériel à l'immatériel dans le droit des biens. Les ressources du langage juridique », in *Le droit et l'immatériel, Archives de philosophie du droit*, t. 43, p. 65.

- J. Hameau et al., « Why do players buy in-game content? An empirical study on concrete purchase motivations », *Computers in Human Behavior*, vol. 68, mars 2017, p. 538.
- B. Haas, « Chinese man "marries" robot he built himself », article *theguardian.com* du 4 avril 2017
- G. Haas, A. Dubarry, M. D'auvergne et R. Ruimy, « Enjeux et réalités juridiques des objets connectés », *Dalloz IP/IT*, 2016, p. 394
- E. Haroff, « France Telecom opens European Backbone Network », article *lightwaveonline.com* du 1er février 2000.
- P. Hérard, « Délit de consultations de sites Internet : une loi inapplicable ? », article du 18/07/16 sur *information.tv5monde.com*.
- V. Hermann, « WannCrypt : une infection "jugulée", le point sur la situation », article *nextinpact.com* du 15 mai 2017.
- O. Hielle, « La technologie Blockchain : une révolution aux nombreux problèmes juridiques », *Dalloz actu.*, 31 mai 2016.
- A. Higgins, « It's France's turn to worry about election meddling by russia », article *nytimes.com* du 17 avril 2017.
- P. Hilt, « L'animal de compagnie lors de la séparation du couple », *AJ Famille*, 2012, p. 74.
- K. Hottot, « The DAO : un pirate dérobe 50 millions de dollars, la contre-attaque se prépare », article *nextinpact.com* du 22 juin 2016.
- K. Hottot, « Ethereum : un "hard fork" controversé pour oublier the DAO », article *nextinpact.com* du 20 juillet 2016.
- J. James, « Date never sleeps 4.0 », article *domo.com* du 28 juin 2016.
- F. Joignot, « Sur Internet, l'invisible propagande des algorithmes », article *lemonde.fr* du 15 septembre 2016.
- J. Julien, V° « Responsabilité du fait d'autrui », in *Rép. civ. Dalloz*, juin 2016.
- A. Kalamar, « Sharewashing is the New Greenwashing », article *opednews.com*, 2013.
- S. Kovacs, « Israël Nisand : la pornographie éduque les enfants à notre place », *lefigaro.fr*, 8 juillet 2015.
- D. Kravets, « Odd lawquit fails to ding FedEx for allowing copies of CC-licensed material », article *arstechnica.com* du 27 février 2017
- M. D. Kudlick, « Host names on-line », 10 janvier 1974 : <https://tools.ietf.org/html/rfc608>.
- V. Kumar, « Make freemium work », *Harvard Business Review*, mai 2014.
- Laboratoire national de métrologie et d'essais, dossier « Longévité des disques enregistrables : mythe ou réalité ? » : <https://www.lne.fr/fr/projets/gis-spadon/longevite-des-disques>.
- D. Larousserie, P. Barthélémy et C. Lesnes, « Après l'élection de Trump, la science entre en résistance », article *lemonde.fr* du 17 avril 2017.
- V. Lasserre, « Investiture de la société civile au Parlement. Analyse d'une nouvelle méthode législative », *JCP G*, 2016, n° 7, 18.

- J. Lasserre-Capdeville, « Le droit régissant le paiement par Internet en France », *RLDA*, 2012, n° 73, p. 84.
- M. Latina, « Contrat : généralités » in *Répertoire civil Dalloz*, mai 2017, n° 1.
- A. Latreille et T. Maillard, « Mesures techniques de protection et d'information », fasc. 1660 in *J-Classeur Propriétaire littéraire et artistique*, 16 février 2015.
- C. Laverdet, « Bitcoins et autres cryptomonnaies : enjeux et défis juridiques », in *Les biens numériques*, éd. Ceprisca, 2015, p. 33.
- A. Lecourt, « Quelles pistes juridiques pour encadrer l'économie collaborative ? », *RLDA*, N° 117, juillet 2016.
- A.-V. Le Fur, « Enfin un cadre juridique pour le crowdfunding, une première étape dans la réglementation », *D.*, 2014, p. 1831.
- D. Legeais, « La blockchain », *RTD. com.*, 2016, p. 830.
- D. Legeais, « Blockchain », fasc. 534 in *J.-Cl. commercial*, mars 2017, n°15.
- D. Leloup, « DuckDuckGo, le petit moteur de recherche qui monte », article *lemonde.fr* du 20 février 2002.
- D. Leloup, « Le même, ou l'art du détournement historique sur Internet », article *lemonde.fr* du 1er mai 2012.
- N. Lenois et A. Jacquinn, « Référencement en ligne et abus de position dominante : quelles problématiques pour plateformes rmes numériques ? », *AJ contrats d'affaires — concurrence — distribution*, 2016, p. 223.
- A. Lepage, « La notion de communauté d'intérêts à l'épreuve des réseaux sociaux », *CCE*, 2013, n° 7, p. 43
- A. Lepage, « Personnalité (Droits de la) » in *Rép. civ. Dalloz*, octobre 2016.
- A.M. Leroyer, « La notion d'état des personnes », in *Mélanges M. Gobert*, Economica, 2004, p. 253.
- F. Lesaulnier, « La définition des données à caractère personnel dans le règlement général relatif à la protection des données personnelles », *Dalloz IP/IT*, 2016, p. 573
- L. Lessig, « Laws that choke creativity », conférence TED mars 2007.
- C. Le Stanc, « Logiciel : trente ans entre droit d'auteur et brevet. Bilan ? », in *Droit et techniques. Etudes à la mémoire du professeur Xavier Linant de Bellefonds*, Lexisnexis, 2007, p. 272.
- Ligue des droits de l'Homme, « Carte d'identité électronique : penser le progrès au lieu de le subir... » : http://www.liguedh.be/images/PDF/documentation/documents_thematiques/carte_identite_electronique.pdf.
- B. Louvel, « Allocation du Premier président Bertrand Louvel » in *la jurisprudence dans le mouvement de l'open data. Actes du colloque à la Cour de cassation, 14 octobre 2016*, JCP G, 2017, n° 9, supplément n° 1.
- D. Mainguy, « Regard prédictif sur la justice prédictive », note de blog du 14 mars 2017 sur *daniel-mainguy.fr*.

- O. Maison Rouge (de), « Darkweb : plongée en eaux troubles », *Dalloz IP/IT*, p. 74
- C. Manara et B. Tabaka, « Pour l'insaisissabilité de l'ordinateur familial », *AJ famille*, 2008, p. 207.
- A. Marcinkowski et J. Wilgaux, « Automates et créatures artificielles d'Héphaïstos : entre science et fiction », *Techniques et culture*, n° 43-44, 2004.
- L. Magid, « It pays to read license agreements », article *pcpitstop.com*, date non précisée.
- J.-P. Marguénaud, « La personnalité juridique des animaux », *D.*, 1998, 205.
- J. Marin, « La nouvelle console de Microsoft sous le feu des critiques », article *lemonde.fr* du 10 juin 2013.
- L. Marino, « Le droit d'accès à Internet, nouveau droit fondamental », *D.*, 2009, p. 2045.
- L. Marino, « Notre vie privée : des little data aux big data », *JGP G*, 2012, n° 47.
- L. Marino, « Comment mettre en œuvre le “droit à l'oubli” numérique ? », *D.*, 2014, p. 1680.
- »L. Marino, « Responsabilité civile et pénale des fournisseurs d'accès et d'hébergement » fasc. 670, in *J.-Cl. Communication*.
- G. Marraud des Grottes, « La blockchain : un secteur encore en phase d'exploration, mais très prometteur... », *RLDI*, 2017, n° 138.
- N. Martial-Braz, « Les nouveaux droits des individus consacrés par la loi pour une République numérique. Quelles innovations ? Quelle articulation avec le Règlement européen ? », *Dalloz IP/IT*, 2016, p. 525.
- N. Martial-Braz et J. Rochfeld, « Les moteurs de recherche, maîtres ou esclaves du droit à l'oubli numérique ? Acte II : le droit à l'oubli numérique, l'éléphant et la vie privée », *D.*, 2014, p. 1481.
- F. Mattatia, « L'usurpation d'identité sur Internet dans tous ses états », *RSC*, 2014, p. 331.
- L. Maurel, « Le CNNum s'est prononcé contre l'instauration d'un droit de propriété privée sur les données personnelles », article *scinfolex.com* du 19/06/14.
- L. Maurel, « Valve et le casse-tête de la monétisation des usages transformatifs », article *scinfolex.com* du 15 mai 2015.
- L. Maurel, « Pourquoi nous avons besoin d'un droit de citation audiovisuelle », article *scinfolex.com* du 17 octobre 2015.
- L. Maurel, « L'exception TDM dans la loi numérique : mérites, limites et perspectives », article *scinfolex.com* du 9 novembre 2016.
- L. Maurel, « Enfin un “upgrade” de l'exception de citation dans la prochaine directive sur le droit d'auteur ? », article *scinfolex.com* du 14 février 2017.
- L. Maurel, « Liberté d'expression : Web web européen subira-t-il la “malédiction du Titanic ?” », article *scinfolex.com* du 30 avril 2017.
- L. Maurel, « Quand la clause Non-Commercial des licences Creative Commons passe en justice », article *scinfolex.com* du 8 mars 2017.
- E. Mechaber, « President Obama urges FCC to implement stronger net neutrality rules », article du 10 novembre 2014, *obamawhitehouse.archives.gov*.

- M. Mekki, « Le formalisme électronique : la “neutralité technique” n’emporte pas “neutralité axiologique” », *RDC*, 2007, n° 3, p. 681.
- A. Mendoza-Caminade, « Le droit confronté à l’intelligence artificielle des robots : vers l’émergence de nouveaux concepts juridiques ? », *D.*, 2016, p. 445.
- W. Mérancourt, « Avec WikiTribune, un cofondateur de Wikipédia s’attaque aux “fake news” », article *letemps.ch* du 28 avril 2017.
- C. Metz, « Before Google and Godaddy, there was Elizabeth Feinler », article *wired.com* du 18 juin 2012.
- C. Metz, « Why does the net still work on christmas ? Paul Mockapetris », article *wired.com* du 23 juillet 2012.
- J. G. McGann, « 2014 Global Go To Think Tank Index Report » (2015) : http://repository.upenn.edu/cgi/viewcontent.cgi?article=1008&context=think_tanks.
- A. Mirsky et K. Tummarello, « Are Retweets Endorsements?: Disclaimers and Social Media », article *dmlp.org* du 4 mai 2012.
- C. Mouly-Guillemaud, « La sentence “nul ne peut se constituer de preuve à soi-même” ou le droit de la preuve à l’épreuve de l’unilatéralisme », *RTD. civ.*, 2007, p. 253.
- J.-L. Mouralis, V° Preuve (1° modes de preuve), in *Rép. civ. Dalloz*, avril 2017.
- J.-L. Mouralis, V° « Preuve (2° règles de preuve », in *Rép. civ. Dalloz*, avril 2017.
- Y. Moreau et C. Dornbierer, « Enjeux de la technologie de blockchain », *D.*, 2016, p. 1856.
- S. Moreil, « Economie collaborative : alternative au capitalisme ou ubérisation de l’économie ? », *Cahiers de droit de l’entreprise*, mai 2017, n° 3, dossier 10.
- Michael D. Murray, « What is Transformative? An Explanatory Synthesis of the Convergence of Transformation and Predominant Purpose in Copyright Fair Use Law », 11 *Chi. -Kent J. Intell. Prop.*, 260, 2012.
- S. Nadia McDonald, « John Olivier's neut neutrality rant may have caused FCC site crash », article *washingtonpost.com* du 4 juin 2014.
- G. Nasri, « Solving information asymmetry: how today’s companies are empowering consumers and creating more efficient markets », article *huffingtonpost.com* du 9 septembre 2013.
- D. Noguero, « L’acceptation dans le contrat électronique », in *Le contrat électronique. Au cœur du commerce électronique, journées d’études organisées par le DJCE de Poitiers*, LGDJ, 2005, p. 49.
- J. A. Obar et A. Oeldorf-Hirsch, « The biggest lie on the internet: ignoring the privacy policies and terms of service policies of social networking services », article du 25 août 2016 disponible sur *papers.ssrn.com*.
- N. Ochoa, « Pour en finir avec l’idée d’un droit de propriété sur ses données personnelles : ce que cache véritablement le principe de libre disposition », *RFDA*, 2015, p. 1157.
- G Orain, « Sur Amazon Turk, les forçats du clic », article *lemonde.fr/pixels* du 22 mai 2017.
- W. Oremus (trad. A. Bourguilleau), « Voici comment fonctionne l’algorithme de Twitter », article *slate.fr* du 10 mars 2017.

- A. Pai, « Statement on the release of senate report on how the white house bowled over FCC independence », *FCC news*, 1er mars 2016.
- P. Pailler, « L'intermédiation en question. L'apport des FinTechs au droit bancaire », *RDBF*, n° 2, mars 2017, dossier 12.
- T. Pasquier, « Le droit social confronté aux défis de l'ubérisation », *Dalloz IP/IT*, 2017, p. 368.
- A. Penneau, « La signature électronique. Rapport de droit français », *RLDI*, 2009, n° 52, supplément spécial, p. 36, n° 19.
- A. Penneau, « La preuve des actes électroniques en droit français. Conséquences du règlement européen e-IDAS », *JCP E*, n° 20, 18 mai 2017, 1264.
- J. W. Penney, « Chilling effects : online surveillance and Wikipédia use », *Berkeley Technology Law Journal*, 2016, vol : 31:1, p. 117.
- G. Pépin, « Trump nommé un ennemi de la neutralité du Net à la tête de la FCC », article *nextinpact.com* du 24 janvier 2017.
- G. Pépin, « “Fake news” : Facebook va rémunérer des éditeurs français et fait sa publicité dans la presse », article *nextinpact.com* du 26 avril 2017.
- G. Pépin, « Sur Ethereum, une plateforme décentralisée de craquage de mots de passe », article *nextinpact.com* du 4 août 2017.
- R. Perray, « La délimitation territoriale du RGPD : le champ d'application et les transferts de données hors de l'Union européenne », *Dalloz IP/IT*, 2016, p. 581.
- R. Perray et P. Salen, « La Cour de justice, les moteurs de recherche et le droit “à l'oubli numérique” : une fausse innovation, de vraies questions », *RLDI*, nov. 2014, n° 109, p. 35
- R. Perray et J. Uzan-Naulin, « Existe-t-il encore des données non personnelles ? », *Dalloz IP/IT*, 2017, p. 286.
- J. Perry Barlow, « A Declaration of the Independence of Cyberspace », 1996, consultable sur www.eff.org/cyberspace-independence.
- A. Petit, « Visite guidée du Darkweb cybercriminel », *Dalloz IP/IT*, 2017, p. 86.
- T. Picard, « Le poids économique direct de la culture en 2015 », *Cultures-chiffres*, 2017, n° 1, consultable sur www.culturecommunication.gouv.fr.
- U. Pidaparthi, « What you should know about iTunes' 56-page legal terms » article *cnn.com* du 6 mai 2011.
- T. Piette-Coudol, « L'identité des personnes, les certificats et la signature électronique », *CCE*, janv. 2005, étude 2.
- M. Popova, « Steve jobs on why computers are like a bicycle for the mind (1990) », article *brainpickings.org* du 21 décembre 2011.
- Y. Pouillet et A. Rouvroy, « Le droit à l'autodétermination informationnelle et la valeur du développement personnel. Une réévaluation de l'importance de la vie privée pour la démocratie. », in *État de droit et virtualité*, K. Benyekhlef & P. Trudel (dir.). Montréal : Thémis, 2009.
- G. Poupard, « évaluation des mesures législatives relatives à la cryptographie », article *liberation.fr* du 24 mars 2016.

- R. Prudent, « Arcade City : l'appli qui rêve d'ubériser Uber », article *tempsreel.nouvelobs.com* du 18 février 2016.
- M. Quémener, « Sites Internet. Retrait, blocage, déréférencement », fasc. 690 in *JurisClasseur communication*, 24 mai 2016.
- M. Rees, « Loi numérique : les députés disent non au domaine commun informationnel », article *nextinpact.com* du 21 janvier 2016.
- J. R. Reidenberg, « Lex informatica : the formulation of information policy rules through technology », *Texas Law Review*, n° 76, 553 (1997-1998)
- J. Rochfeld, « La loi n° 2004-575 du 21 juin 2004 pour la confiance en l'économie numérique », *RTD. civ.*, 2004, p. 574.
- J. Rochfeld, « Contre l'hypothèse de la qualification des données personnelles comme des biens », in *Les biens numériques*, Ceprisca, 2015, p. 226
- J. Rochfeld et C. Zolynski, « La “loyauté” des “plateformes”. Quelles plateformes ? Quelle loyauté ? », *Dalloz IP/IT*, 2016, p. 520.
- J. Rochfeld, « Le “contrat de fourniture de contenus numériques” : la reconnaissance de l'économie spécifique “contenus contre données” », *Dalloz IP/IT*, 2017, p. 15.
- F. Rouvière, « La justice prédictive, version moderne de la boule de cristal », *RTD. civ.*, 2017, p. 527.
- M. Rose, « Chasing the Whale: Examining the ethics of free-to-play games », article *gamasutra.com* du 9 juillet 2013.
- J.H. Saltzer, D. P. Reed et D. D. Clarck, « End-to-end arguments in system design », *ACM Transactions on Computer Systems*, vol. 2, issue 4, nov. 1984, p. 277.
- L. Saenko, « Le darkweb : un nouveau défi pour le droit pénal contemporain », *Dalloz IP/IT*, 2017 p. 80.
- A. Schmitt, « Existe-t-il un droit à l'anonymat sur Internet ? », article *unpeuedroit.fr* du 13 décembre 2014.
- F. Schwerer, « Réflexions sur la preuve et la signature dans le commerce électronique », *CCE*, déc. 2000, chron. 16.
- F. Schott, « Les “civic tech ou le b.a-ba de la démocratie 2.0 », article *lemonde.fr* du 26 avril 2017.
- J. Sénéchal, « Ubérisation et droit de la consommation », *Dalloz IP/IT*, 2017, p. 363.
- A. Shalal, « Germany waters down plan for social media fines over hate speech : Der Spiegel », dépêche *Reuters* du 4 avril 2017.
- K. Sheehan, « YODA, the Bill That Would Let You Own (and Sell) Your Devices, Is Re-Introduced in Congress », article *eff.org* du 7 février 2017.
- P. Sirinelli, « Le peer-to-peer devant la Cour suprême », *D.*, 2005, p. 1796.
- E. Steel, C. Locke, E. Cadman et B. Freese, « How much is your personal data worth ? », article *ft.com* du 12/06/13.
- P. Stoffel-Munck, « LCEN. La réforme des contrats du commerce électronique », *CCE*, sept. 2004, étude 30.

- J. Snyder, K. Komaitis et A. Robachevsky, « The history of IANA : an extended timeline with citations and commentary », janvier 2017, p. 2 : <http://www.internetsociety.org/ianatimeline>.
- Mark Stefik, « Epilogue: Choices and Dreams » in *Internet Dreams: Archetypes, Myths, and Metaphors*, Cambridge, Mass.: MIT Press, 1996, 390.
- P. Storrer, « Crowdfunding, bitcoin : quelle régulation ? », *D.*, 2014, p. 832.
- E. Stoycheff, « Under surveillance: examining Facebook's spiral of silence effects in the wake of NSA Internet monitoring », *Journalism & Mass Communication Quarterly*, 2016, vol. 93(2), p. 296.
- P. Svensson, « Comcast blocks some internet traffic », article *The Associated Press*, 19 octobre 2007.
- N. Szabo, « Smart contracts : building blocks for digital markets » : http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart_contracts_2.html.
- M. Szadowski et D. Leloup, « Prism, Snowden, surveillance : 7 questions pour tout comprendre », article *lemonde.fr* du 08/08/13.
- A. Tabarrok et T. Cowen, « The end of asymmetric information ? », article *cato-unbound.org* du 6 avril 2015.
- T. Tierranova, « Free labor : producing culture for the digital economy », *Social Text*, 63 (Volume 18, Number 2), Summer 2000, p. 33/
- C. Torres, « Le credit scoring : une pratique très encadrée par la CNIL », *Gaz. Pal.*, 24/07/10, n° 205.
- A. Touati, « Tous les contrats ne peuvent pas être des smart contracts », *RLDC*, 2017, n° 147.
- J. Toussay, « Pour la première fois, "l'homme à la pelle" témoigne... », article *huffingtonpost.fr* du 9 février 2017.
- M. Tual, « Absurde, créatif et débauché : dix ans après, "Second Life" est toujours bien vivant », article *lemonde.fr/pixels* du 28 avril 2016.
- A. M. Turing, « On computable numbers, with an application to the Entscheidungsproblem » : https://www.cs.virginia.edu/~robins/Turing_Paper_1936.pdf.
- M. Untersinger, « Terrorisme : pour contourner le chiffrement des messages, Bernard Cazeneuve en appelle à l'Europe », article *lemonde.fr* du 23/08/16.
- M. Untersinger, « Lawrence Lessig : "Le problème de la démocratie actuellement c'est qu'elle n'est pas représentative" », article *lemonde.fr* du 23 avril 2017.
- C. R. Vance, F. Molins, A. Leppard et J. Zaragoza, « When phone encryption blocks justice », article *nytimes.com* du 11/08/15.
- V. Varnerot, « La circulation des œuvres numériques » in *Les biens numériques*, éd. Ceprisca, 2014, p. 109.
- T. Verbiest, « Technologies de registre distribué (blockchain) : premières pistes de régulation », *RLDI*, 2016, n° 129.
- T. Verbiest, « Quelle valeur juridique pour les smart contracts ? », *RLDA*, 2017, n° 129.

- M. Videau, « Aspect techniques de la preuve littérale reposant sur l'écrit électronique », *RLDI*, 2009, n° 52, supplément spécial, p. 15.
- L. Vinogradoff, « Le créateur de Pepe The Frog tue sa grenouille, contaminée par l'extrême-droite », article *Le Monde Big Browser* du 8 mai 2017.
- J. Weinberg, « ICANN and the problem of legitimacy », *Duke law journal*, vol. 50:187, p. 187.
- A. Williams, « How Facebook can affect your credit score », article *ft.com* du 25/08/16.
- T. Wu, « Network neutrality, broadband discrimination », *Journal of Telecommunications and High Technology Law*, Vol. 2, p. 141, 2003.
- F. Zénati, « L'immatériel et les choses » , in *Le droit et l'immatériel*, *Archives de philosophie du droit*, t. 43, p. 79.
- C. Zolynski, « La gratuité en questions », in *La gratuité. Un concept aux frontières de l'économie et du droit*, LGDJ, 2013, p.XI.
- C. Zolynski, « La Privacy by design appliquée aux objets connectés : vers une régulation efficiente du risque informationnel ? », *Dalloz IP/IT*, 2016, p. 404.
- C. Zolynski, « Blockchain et smart contracts : premiers regards sur une technologie disruptive », *RDBF*, n° 1, janvier 2017, dossier 4
- C. Zolynski, « La blockchain : la fin de l'ubérisation ? », *Dalloz IP/IT*, 2017, p. 385.

IV - Rapports, avis, publications institutionnelles

- ANSSI, *Guide d'hygiène informatique*, version 2.0, janvier 2017.
- ARCEP, *Rapport au Parlement et au Gouvernement sur la neutralité de l'internet*, sept. 2012.
- ARCEP, *L'état d'internet en France édition 2017*, mai 2017.
- ARCEP, *Equipements terminaux. Analyse de leur influence sur l'ouverture de l'internet*, 30 mai 2017.
- AMF et ACPR, *Guide du financement participatif à destination des plate-formes et porteurs de projets*, 14 mai 2013.
- V.-L. Bénabou (prés.) et D. Botteghi (rapp.), *La mise à disposition ouverte des œuvres de l'esprit*, rapport CSPLA, juin 2007.
- V.-L. Bénabou (présidente) et F. Langrognet (rapporteur), *Rapport de la mission du CSPLA sur les « oeuvres transformatives »*, 2014.
- BEREC, *Guidelines on the Implementation by National Regulators of European Net Neutrality Rules*, 30 août 2016.
- M. Bouvard et al., *Sur l'économie collaborative : propositions pour une fiscalité simple, juste et efficace*, *Rapport d'information du Sénat n° 690 fait au nom de la commission des finances*, 17 septembre 2015.
- G. Braibant, *Données personnelles et société de l'information. Rapport au Premier ministre sur la*

transposition en droit français de la directive n° 95/46, décembre 1998, p. 13.

L. Cadiet (dir.), *L'open data des décisions de justice. Mission d'étude et de préfiguration sur l'ouverture au public des décisions de justice*, Rapport à Mme la garde des Sceaux, ministre de la Justice, novembre 2017.

CNCDH, *Avis sur la lutte contre les discours de haine sur internet*, 12 février 2015.

CNIL, *Communication relative à la mise en œuvre de dispositifs de reconnaissance par empreinte digitale avec stockage dans une base de données*, date non précisée.

CNIL, *Mort numérique : peut-on demander l'effacement des informations d'une personne décédée ?*, publication du 29/10/14

CNIL, *Mobilitics, saison 2 : nouvelle plongée dans l'univers des smartphones et de leurs applications*, publication du 15/12/14.

CNIL, *Délibération n° 2015-414 du 19 novembre 2015 portant avis sur un projet de la loi pour une République numérique*, p. 18.

CNIL, *Les enjeux de 2016 (3) : quelle position de la CNIL en matière de chiffrement ?*, avril 2016.

CNIL, *Pack de conformité véhicules connectés*, octobre 2017.

CNNum, *Rapport relatif à l'avis net neutralité n° 2013-1 du 1er mars 2013*.

CNNum, *Neutralité des plateformes. Réunir les conditions d'un environnement numérique ouvert et soutenable*, mai 2014.

CNNum, *Avis n° 2014-3 du 15 juillet 2014 sur l'article 9 du projet de loi renforçant les dispositions relatives à la lutte contre le terrorisme*.

CNNum, *Avis n° 2015-3 relatif au projet de loi pour une République numérique*, novembre 2015.

CNNum, *Rapport Travail, emploi, numérique. Les nouvelles trajectoires*, janvier 2016.

CNNum, *Avis sur le fichier TES*, décembre 2016.

CNNum, *La confiance dans la vie publique, avec et pour les citoyen-ne-s d'une société numérique*, avis de juillet 2017.

CNNum, *Rapport Prédictions, chiffrement et libertés*, septembre 2017.

Comité économique et social européen, *L'intelligence artificielle*, avis d'initiative du 31 mai 2017.

Commission européenne, *Communication au Parlement européen, au Conseil, au Comité économique et social européen et au Comité des régions du 19 avril 2011 sur l'Internet ouvert et la neutralité d'Internet en Europe*.

Commission européenne, *Lignes directrices sur l'application de la directive 2004/113/CE du Conseil dans le secteur des assurances, à la lumière de l'arrêt de la Cour de justice de l'Union européenne dans l'affaire C-236/09 (Test-Achats)*, texte 2012/C 11/01, JOUE.

Commission européenne, *Communication au Parlement européen, au Conseil, au Comité économique et social européen et au Comité des régions, Libérer le potentiel du financement participatif dans l'Union européenne*, 27 mars 2014.

Commission européenne, *Un agenda européen pour l'économie collaborative*, COM.(2015) 356, 2

juin 2016.

Conseil d'Etat, *Le numérique et les droits fondamentaux*, La documentation française, 2014.

Conseil d'État, *Puissance publique et plateformes numériques : accompagner l'« ubérisation »*, La documentation française, 2017.

Conseil général de l'économie, *Modalités de régulation des algorithmes de traitement des contenus*, rapport de mai 2016.

Crown Prosecution Service, *Guidelines on prosecuting cases involving communications sent via social media*, version 2016.

C. Erhel et L. de La Raudière, *Rapport d'information sur la neutralité de l'internet et des réseaux*, enregistré à la Présidence de l'Assemblée nationale le 13 avril 2011.

FCC, *Report and Order. Preserving the Open Internet Broadband Industry Practices*, 10-201, 21 décembre 2010.

FCC, *Report and order on remand, declaratory ruling, and order*, 15-24, 12 mars 2015.

FCC, *Restoring Internet freedom. Notice of proposed rulemaking*, 17-60, 23 mai 2017.

FCC, *Declaratory ruling, Restoring Internet Freedom, report and order*, FCC 17-166.

Fédération e-commerce et vente à distance (FEDAV), *Les chiffres clés 2016/2017*.

France Diplomatie, *Gouvernance de l'internet - réforme de l'ICANN*, publication du 10 mars 2016.

G29, *Déclaration du G29 relative à la décision de la Commission européenne concernant le Privacy Shield (bouclier de protection des données UE-États-Unis)*, 29 juillet 2016.

G29, *Guidelines on consent under regulation 2016/679*, novembre 2017.

G29, *Statement of the WP29 on encryption and their impact on the protection of individuals with regard to the processing of their personal data in the EU*, avril 2018.

Groupe de travail interministériel sur la lutte contre la cybercriminalité, *Protéger les internautes. Rapport sur la cybercriminalité*, juillet 2014.

HADOPI, *Bulletin d'information trimestriel n° 2 - chiffres clés de la réponse graduée*, février 2017.

ICANN, *Guide d'initiation à l'ICANN*, non daté.

ICANN, *Major milestone for the internet and ICANN. The Key Signing ceremony is now complete*, publication icann.org du 16 juin 2010.

ICANN, *ICANN, Revised ICANN bylaws and restated articles of incorporation*.

Internet association, *An open letter to Congress from U.S. Business*, 2016.

M. Joulaud (rapp.), *Projet d'avis de la commission de la culture et de l'éducation sur la proposition de directive du Parlement européen et du Conseil sur le droit d'auteur dans le marché unique numérique*, 6 février 2017, 2016/0280 (COD).

P. Lescure (dir.), *Contribution aux politiques culturelles à l'ère numérique*, t. 1, 2013.

Library of Congress, Copyright office, 37 CFR Part 201, *Exemption to prohibition on circumvention of copyright protection systems for access control technologies*, Federal Register vol.

75, n° 143, 27 juillet 2010.

A. Linden, *Rapport d'activité 2015 de la personnalité qualifiée prévue par l'article 6-1 de la loi n° 2004-575 du 21 juin 2004 créé par la loi n° 2014-1353 du 13 novembre 2014 renforçant les dispositions relatives à la lutte contre le terrorisme*, mars-février 2016.

C. Morin-Desailly, *L'Europe au secours de l'Internet : démocratiser la gouvernance de l'Internet en s'appuyant sur une ambition politique et industrielle européenne*, Rapport d'information du Sénat n° 696 fait au nom de la Mission commune d'information sur la gouvernance mondiale de l'Internet, déposé le 8 juillet 2014.

NTIA, *NTIA announces intent to transition key internet domain name functions*, 14 mars 2014.

NTIA, *Statement of assistant secretary Strickling on IANA functions contract* ; 1^{er} oct. 2016.

Observatoire de la sécurité des cartes de paiement, *Rapport annuel 2015*.

Observatoire des libertés et du numérique, *Chiffrement, sécurité et libertés. Positionnement de l'Observatoire des libertés et du numérique*, janvier 2017.

Parlement européen, *Résolution sur l'Internet ouvert et la neutralité d'internet en Europe*, 17 novembre 2011.

Parlement européen, *Résolution sur un agenda européen pour l'économie collaborative*, 2017/2003(INI), 15 juin 2017.

F. Pillet et T. Mohamed Soilihi, *L'équilibre de la loi du 29 juillet 1881 à l'épreuve d'Internet. Rapport d'information fait au nom de la commission des lois*, n° 767.

Quadrature du Net (la), *Eléments pour la réforme du droit d'auteur et des politiques culturelles liées*, non daté.

Quadrature du net (la), *Dépôt des plaintes collectives contre les GAFAM !*, publication du 28 mai 2018 sur laquadrature.net.

J. Reda, membre de la commission des affaires juridiques du Parlement européen, *Rapport sur la mise en œuvre de la directive 2001/29/CE du Parlement européen et du Conseil du 22 mai 2001 sur l'harmonisation de certains aspects du droit d'auteur et des droits voisins dans la société de l'information*, 24 juin 2015 (2014/2256 (INI)).

S. Riocreux, *Rapport sur la proposition de loi relative à l'extension du délit d'entrave à l'interruption volontaire de grossesse*, fait au nom de la commission des affaires sociales du Sénat, n° 183, 6 décembre 2016.

P. Sirinelli, J.-A. Benazeraf et A. Bensamoun, *Mission droit de communication au public. Rapport et propositions*, Conseil supérieur de la propriété littéraire et artistique, décembre 2016.

P. Terrasse (dir.), *Rapport au Premier ministre sur l'économie collaborative*, février 2016.

Table des matières

Remerciements.....	3
Liste des principales abréviations.....	5
Sommaire.....	9
Introduction.....	11
I - Le numérique.....	13
A - Les machines.....	14
B - Les réseaux.....	19
II - Le numérique et le droit.....	23
A - Les rapports de collaboration.....	24
1 - L'accès à l'information.....	24
2 - L'analyse de l'information.....	28
3 - Les actions automatisées.....	31
B - Les rapports de concurrence.....	32
C - Les rapports de soumission.....	37
Première notion - La personne.....	41
Chapitre 1 - L'identité numérique.....	47
Section 1 - Les éléments de l'identité numérique.....	51
I - Le centre : l'identité stable.....	51
A - L'identité occultée.....	52
B - L'identité prouvée.....	56
II - La périphérie : l'identité construite.....	66
A - La naissance de l'identité construite.....	67
B - La montée en puissance de l'identité construite.....	69
1 - Une collecte généralisée.....	69
2 - Des traitements à grande échelle.....	75
Section 2 - La protection de l'identité numérique.....	78
I - La protection plancher exigée des responsables de traitement.....	85
A - La collecte des données.....	85
B - L'exploitation des données.....	93
C - La circulation des données.....	98
D - Autorités de contrôle et sanctions.....	102
II - La gestion personnalisée accessible aux individus.....	104
A - En amont de la collecte de données.....	105
1 - La collecte rationnée.....	105

2 - La collecte empêchée.....	110
a – Le contenu des données.....	110
b – Les parties à une communication.....	115
B – En aval de la collecte de données.....	119
1 - La nature du droit de l'individu sur ses données.....	120
a – Les théories réalistes.....	120
b – Les théories personnalistes.....	123
2 - Les composantes du droit de l'individu sur ses données.....	126
a – Le droit de connaître ses données.....	126
b – Le droit de faire modifier ou supprimer ses données.....	127
c - Le droit au déréférencement (dit « droit à l'oubli »).....	128
d - Le droit de récupérer ses données.....	134
e – Le droit de transmettre ou non ses données après sa mort.....	137

L'identité numérique : conclusion.....144

Chapitre 2 - La communication électronique.....146

Section 1 – La production de l'information.....153

I – Les difficultés tenant à la détermination de l'expression illicite.....	154
A – L'expression personnelle.....	155
1 - Le caractère anonyme du propos.....	157
2 - Le caractère privé du propos.....	160
B - L'expression relayée.....	164
1 - La création d'un lien hypertexte.....	165
2 - Les fonctions de partage des réseaux sociaux.....	169
3 - Les boutons exprimant une « émotion » face à un contenu.....	174
II - Les difficultés tenant à la sanction de l'expression illicite.....	176
A - La brièveté des délais de prescription.....	176
1 - La prescription applicable à la publication initiale.....	177
2 - La prescription applicable aux publications ultérieures.....	181
B - L'abondance de contenus illicites.....	184

Section 2 - La canalisation de l'information.....186

I - La suppression de l'information.....	188
A - Le retrait de contenus par les intermédiaires techniques après signalement.....	193
B - Le blocage d'un site Internet par les fournisseurs d'accès.....	201
II - L'agencement de l'information.....	205
A - La personnalisation des contenus.....	208
B - La véracité des contenus.....	213

La communication numérique : conclusion.....219

Deuxième notion - La propriété.....221

Section 1 - Les infrastructures.....225

I – La télécommunication.....	226
-------------------------------	-----

A – La tentation privée : discriminer les flux.....	227
1 – La neutralité des origines.....	228
2 – La montée des discriminations.....	231
B – La réaction publique : imposer la neutralité du réseau.....	235
1 – La faveur européenne.....	235
2 – Le revirement américain.....	240
II – La coordination.....	244
A – La naissance de l’ICANN : une structure privée américaine au pouvoir mondial.....	246
B – L’évolution de l’ICANN : la gestion d’un commun par le consensus ?.....	250
Section 2 – Les contenus.....	256
I – Le droit sur les œuvres.....	259
A – La propriété protégée.....	259
1 – La résistance au numérique.....	259
a – La circulation non transformative.....	260
b – La circulation transformative.....	273
2 – L’exploitation du numérique.....	287
a – Une protection étendue à de nouveaux objets.....	287
b – Une protection renforcée par de nouveaux moyens.....	291
B – La propriété tempérée.....	298
1 – Les tempéraments légaux.....	298
2 – Les tempéraments volontaires.....	301
II – Le droit sur les copies d’œuvres.....	307
A – La disparition progressive des supports.....	307
B – Le maintien artificiel des copies.....	314
Section 3 – Les terminaux.....	321
La propriété : conclusion.....	329
Troisième notion – Le contrat.....	333
Section 1 – Droit commun des contrats.....	336
I – L’idéal de fluidité dans la conclusion des contrats.....	336
A – La fragilité du consentement au contrat.....	336
1 – La complexité des offres.....	337
a – L’économie générale du contrat : des gratuités factices.....	338
b – Les stipulations détaillées : l’omniprésence de clauses trompeuses.....	341
2 – La simplicité de l’acceptation.....	345
B – La fragilité des preuves du contrat.....	350
1 – La place marginale de la preuve littérale électronique.....	353
2 – La place centrale des modes de preuve imparfaits.....	359
a – Simplicité.....	360
b – Faiblesses.....	368
Alpha – La fraude criminelle.....	370
Bêta – La fraude familiale.....	374
II – L’idéal de rigueur dans l’exécution des contrats.....	379

A – Les moyens de l'exécution automatisée.....	379
B – Les risques de l'exécution automatisée.....	382
Section 2 – Droits spéciaux des contrats.....	386
I – Les contrats d'intermédiaire.....	390
A – Les plateformes en dehors du marché : une fonction d'entremise.....	391
1 – Le principe : l'entremise au profit du marché.....	391
2 – La limite : la direction du marché.....	395
B – Les plateformes au-dessus du marché : le régime du courtage.....	397
1 – Les informations relatives à la plateforme.....	398
2 – Les informations relatives au contrat projeté.....	402
II – Les contrats intermédiés.....	405
A – La remise en cause du contrat de travail.....	407
1 – De nouvelles formes d'activité.....	407
2 – De nouvelles formes de protection.....	410
B – La remise en cause du contrat de consommation.....	413
1 – Le discours des fournisseurs.....	414
2 – La surface financière des fournisseurs.....	416
Le contrat : conclusion.....	418
Bibliographie.....	421
I – Ouvrages généraux.....	421
II - Ouvrages spéciaux, thèses, monographies.....	422
III - Articles, fascicules.....	424
IV - Rapports, avis, publications institutionnelles.....	437
Table des matières.....	441