Université de Lille
Faculté des Sciences Juridiques, Politiques et Sociales

# VERS UN ENCADREMENT DES SYSTÈMES DE RECOMMANDATION

Mémoire de recherche dans le cadre du Master 2
*Droit du cyberespace : technologies et innovation numérique*
Année universitaire 2020 - 2021

**Sebastien LELEU**

Sous la direction de Monsieur Marcel MORITZ

*Les opinions exprimées dans ce mémoire sont propres à leur auteur et n'engagent pas l'Université de Lille*.

# REMERCIEMENTS

J’adresse mes plus sincères remerciements à mon directeur de mémoire et de formation, Monsieur Marcel MORITZ. La qualité de sa formation, de ses enseignements, et de son accompagnement tout au long de ces deux années ont été des plus précieux pour moi.

Mes remerciements sont également adressés à Audrey DEQUESNES et Laurène BAUDOUIN, pour leur soutien chaleureux tout au long de mon stage au sein du CERAPS.

Je remercie aussi tous les enseignants ayant participé à cette formation, pour leur bienveillance à notre égard, et leurs riches enseignements.

Je tiens à remercier plus personnellement mes proches de la Team Cévennes pour leur soutien indéfectible tout au long de mes études, et avec qui les années universitaires ont été les plus palpitantes que je puisse espérer.

Au Rituel, j’adresse mes sentiments les plus distingués.

À ma mère, j’adresse ma profonde affection.

Enfin, je remercie vivement Léa, Tilila, et Ines, qui ont contribué à la relecture de ce mémoire, et plus largement à son accomplissement.

# LISTE DES ABREVIATIONS

| | |
|---|---|
| Aff. | Affaire |
| AFP | Agence France Presse |
| *AJCT* | *Actualité juridique des collectivités territoriales* |
| *AJDA* | *Actualité juridique de droit administratif* |
| ANSSI | Agence nationale de la sécurité des systèmes d'information |
| ARCEP | Autorité de régulation des communications électroniques, des postes et de la distribution de la presse |
| ARCOM | Autorité de régulation de la communication audiovisuelle et numérique |
| Art. | Article |
| BATX | Baidu, Alibaba, Tencent, Xiaomi |
| c/ | Contre |
| C. civ. | Code civil |
| C. consomm. | Code de la consommation |
| C. élect. | Code électoral |
| Cass. | Cour de cassation |
| CCDH | Center for Countering Digital Hate |
| *CCE* | *Communication commerce électronique* |
| CE | Conseil d'État |
| CESDH | Cour européenne des droits de l'homme |
| CEPD | Contrôleur européen de la protection des données |
| Cf. | Conférer, consulter |
| Ch. | Chambre |
| Civ. | Cassation, chambre civile |
| CJA | Code de justice administrative |
| CJCE | Cour de justice des communautés européennes |
| CJUE | Cour de justice de l'Union européenne |
| CNDCH | Commission nationale consultative des droits de l'homme |
| CNIL | Commission nationale de l'informatique et des libertés |
| Co. | Et compagnie |
| Coll. | Collection |
| Cons. | Considérant |
| Cons. const. | Conseil constitutionnel |
| Chron. | Chronique |
| CSA | Conseil supérieur de l'audiovisuel |
| DACP | Donnée à caractère personnel |
| DC | Décision |

| | |
|---|---|
| DDHC | Déclaration des droits de l'Homme et du citoyen |
| Dir. | Directeur |
| DMA | Digital Market Act |
| DSA | Digital Service Act |
| Ed. | Édition |
| Et al. | Et autres (du latin *et alii*) |
| GAFAM | Google, Apple, Facebook, Amazon, Microsoft |
| *Gaz. Pal.* | *Gazette du palais* |
| HADOPI | Haute autorité pour la diffusion des œuvres et la protection des droits sur Internet |
| IA | Intelligence artificielle |
| *Ibid.* | Au même endroit (du latin *Ibidem*) |
| Inc. | Incorporation |
| IFOP | Institut français d'opinion publique |
| JORF | Journal officiel de la république française |
| LCEN | Loi pour la confiance dans l'économie numérique |
| LGDJ | Librairie générale de droit et de jurisprudence |
| LINC | Laboratoire d'Innovation Numérique de la CNIL |
| OCDE | Organisation de coopération et de développement économiques |
| *Op. cit.* | Œuvre précitée (du latin *opere citato*) |
| p. | Page |
| pp. | Pages |
| *Rev. UE* | *Revue de l'Union européenne* |
| RGPD | Règlement général sur la protection des données |
| *RIDE* | *Revue internationale de Droit économique* |
| *RLDF* | *Revue des droits et libertés fondamentaux* |
| *RLDI* | *Revue Lamy Droit de l'Immatériel* |
| RTB | *Real-time bidding* |
| *RTD Com.* | *Revue trimestrielle de droit commercial* |
| *RTD Eur.* | *Revue trimestrielle de droit européen* |
| *TAL* | *Revue Traitement automatique des langues* |
| TFUE | Traité sur le fonctionnement de l'Union européenne |
| TGI | Tribunal de grande instance |
| TGP | Très grande plateforme |
| UE | Union européenne |
| V. | Voir |
| Vol. | Volume |

# SOMMAIRE

# INTRODUCTION GENERALE

« *Figure-toi des hommes dans une demeure souterraine, en forme de caverne, ayant sur toute sa largeur une entrée ouverte à la lumière. […] La lumière leur vient d'un feu allumé sur une hauteur, au loin derrière eux. […] Penses-tu que dans une telle situation ils n'aient jamais vu autre chose d'eux-mêmes et de leurs voisins que les ombres projetées par le feu sur la paroi de la caverne qui leur fait face ? […] Assurément, de tels hommes n'attribueront de réalité qu'aux ombres* »[1]

À l'image de cette allégorie de la caverne de Platon, l'intérieur représentant le monde de l'opinion tandis que l'extérieur, le monde de la connaissance, est-il possible de détourner le regard de ces ombres déformées afin d'y entrevoir la Vérité ? La perception de l'étendue du monde par les individus n'a fait que croitre siècle après siècle, et a atteint une singularité depuis l'ère de l'information.

L'humain n'a jamais recherché, consommé, et réagi à autant de contenu, d'actualité et d'informations que lors de cette décennie. À l'heure de la rédaction de ce mémoire, chaque seconde équivaut à 9 500 tweets, 1 000 publications sur Instagram, 94 000 recherches sur Google, 90 000 vidéos visionnées sur YouTube, pour un total de 124 000 *Giga Bit* de trafic sur Internet[2]. Ce flux d'informations toujours plus massif s'accompagne de toujours plus d'utilisateurs, environ 53% de la population mondiale étant à présent sur les réseaux sociaux en 2021, et plus généralement, presque 60% du monde est aujourd'hui sur Internet[3].

Les utilisateurs du numérique et la quantité d'informations sont donc conséquents à l'échelle de l'humanité. De quelle manière ces utilisateurs ont-ils donc accès au contenu et à l'actualité ? Les plateformes, et plus particulièrement les réseaux sociaux, ont dorénavant une importance capitale dans ce domaine. En effet, il a été estimé en 2019 que 62% des jeunes internautes

[1] PLATON, *La République Livre VII*, Garnier-Flammarion, Paris, 1987, pp. 273-276, dans : Traduction de BACCOU (R.), « Le récit de l'allégorie de la Caverne », *Horizons philosophiques* [en ligne], vol. 9 n° 2, pp. 21–25, [consulté le 28 juillet 2021].
[2] INTERNET LIVES STATS, 2021 [en ligne], [consulté le 27 juillet 2021].
[3] WE ARE SOCIAL, *Digital 2021 global overview report* [en ligne], rapport de janvier 2021, p. 23, [consulté le 27 juillet 2021].

utilisent les réseaux sociaux pour s'informer[4]. Au-delà d'utiliser internet et les réseaux sociaux pour s'informer, ils sont de surcroit la principale source d'information pour environ 45% des utilisateurs âgés de 18 à 34 ans selon un sondage de l'institut IFOP réalisé la même année[5].

Face à ce constat, il apparait logique de trouver des solutions permettant de trier ce flux d'informations toujours plus massif, en établissant des recommandations et classifications de cette masse de contenu, afin d'afficher les résultats les plus pertinents. Par ailleurs, cette explosion de l'information disponible sur internet s'accompagne d'une augmentation exponentielle des données et traces numériques, données sur lesquelles les GAFAM[6] et BATX[7] reposent en grande partie afin d'assoir leur empire numérique. Ces données, qui peuvent potentiellement être des données à caractère personnel (DACP) au sens du Règlement Général sur la Protection des Données (RGPD)[8], constituent en quelque sorte une nouvelle identité numérique, un profil issu du traitement des données des individus, et dont l'exploitation et la valorisation représentent un nouvel enjeu de taille.

À l'aide de ces données, les systèmes de recommandation ont pu sans cesse s'améliorer, et s'adapter de plus en plus à chaque individu, afin de proposer des méthodes de filtrage permettant de leur soumettre un contenu toujours plus proche de leurs attentes et préférences. Cette précision a permis entre autres de révolutionner le marketing et de mettre en place un processus de publicités ciblées, processus ayant ouvert la voie au succès financier de Google notamment[9]. Eric Schmidt, ancien PDG de Google, avançait bien que « *La technologie va être tellement bonne qu'il sera difficile pour les gens de voir ou de consommer quelque chose qui n'a pas été quelque part ajusté pour eux* »[10].

---

[4] CSA, *Capacité à informer des algorithmes de recommandation : Une expérience sur le service Youtube* [en ligne], rapport de novembre 2019, p. 3, [consulté le 26 juillet 2021].
[5] IFOP, *Enquête sur le complotisme – vague 2* [en ligne], sondage IFOP pour la Fondation Jean-Jaurès et Conspiracy Watch, janvier 2019, p. 16, [consulté le 26 juillet 2021].
[6] Acronyme correspondant à Google, Apple, Facebook, Amazon et Microsoft.
[7] Acronyme correspondant à Baidu, Alibaba, Tencent, Xiaomi.
[8] 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, art. 4, une donnée à caractère personnel est « *toute information se rapportant à une personne physique identifiée ou identifiable* ».
[9] ZUBOFF (S.), *L'âge du capitalisme de surveillance*, Zulma, 2020, p. 98.
[10] ROUVROY (A.), BERNS (T.), « Gouvernementalité algorithmique et perspectives d'émancipation », *Réseaux* [en ligne], vol. 177 n° 1, 2013, pp. 163-196, [consulté le 26 juillet 2021].

Comment ces systèmes fonctionnent-t-ils dans leur globalité ? Avant d'analyser les conséquences issues de l'utilisation de ces recommandations sur internet, il est important d'en comprendre les différents rouages.

## I - LE ROLE PREPONDERANT DES ALGORITHMES D'INTELLIGENCE ARTIFICIELLE DANS LA RECOMMANDATION DU CONTENU

Afin de garantir un fonctionnement optimal de la recommandation du contenu, la plupart des plateformes en ligne utilisent des algorithmes. Dans un rapport de 2017, la Commission Nationale de l'Informatique et des Libertés (CNIL) a pu définir l'algorithme comme étant une « *suite finie et non ambigüe d'instructions permettant d'aboutir à un résultat à partir de données fournies en entrée* », et dans le monde numérique, ces algorithmes combinent « *des informations pour résoudre un problème et produire des résultats* »[11]. L'usage d'algorithmes au sens général n'est pas conditionné à l'utilisation de matériel informatique, une simple recette de cuisine par exemple est un algorithme permettant de produire un résultat attendu à partir d'instructions[12]. Son usage est par ailleurs très ancien, des tablettes vieilles de près de quatre mille ans attestant de l'utilisation d'algorithmes déjà sophistiqués ayant été retrouvées en Mésopotamie[13]. Compléments nécessaires à l'exploitation des données, ces algorithmes appliqués à l'informatique ont de nombreuses applications, que ce soit dans la recommandation de contenu, l'analyse médicale d'images, le calcul de résultats, la prise de décision automatisée, et bien d'autres encore.

Naturellement, une rapide typologie et explication de leur fonctionnement s'impose. Concernant les types de systèmes et leur élaboration, les algorithmes utilisés dans la recommandation sont élaborés à partir de trois méthodes différentes[14]. La première méthode est un *filtrage basé sur le contenu*, consistant à proposer à l'utilisateur un contenu pertinent par rapport à ce qu'il a déjà pu apprécier auparavant. La seconde méthode est le *filtrage collaboratif*, qui consiste soit à croiser les goûts des utilisateurs et les catégoriser dans un cluster

[11] Rapport de la CNIL, *Comment permettre à l'Homme de garder la main ? Les enjeux éthiques des algorithmes et de l'intelligence artificielle*, Décembre 2017, p. 7.
[12] D'ASCOLI (S.), *Comprendre la révolution de l'intelligence artificielle*, Ed. First, 2020, p. 17.
[13] VILLANI (C.), « La mathématique n'est pas qu'une matière abstraite », *in* CHAUVIERE (F.), *Les grandes épopées qui ont fait la science*, Ed. Flammarion, 2020, pp. 255-281.
[14] V. notamment pour une explication des différentes méthodes de filtrage : POIRIER (D.), FESSANT (F.), TELLIER (I.), « De la Classification d'Opinion à la Recommandation : l'Apport des Textes Communautaires », *Revue TAL* [en ligne], Opinions, sentiments et jugements d'évaluation, vol. 51 n° 3, 2010, p. 22, [consulté le 29 juillet 2021].

de goûts communs, ou à rapprocher le contenu apprécié par les mêmes utilisateurs. Amazon est une bonne illustration de l'utilisation de ce système. Enfin, le *filtrage hybride* exploite le potentiel de ces deux méthodes, tout en pouvant faire appel à d'autres données complémentaires, telles que des données démographiques, sociales, et bien d'autres[15]. L'analyse du sociologue Dominique Cardon concorde en substance avec l'approche technique de ces systèmes. Cardon proposait une typologie distinguant quatre familles d'algorithmes en fonction de la métrique de mesure utilisée pour classifier l'importance d'une information, à savoir la popularité, l'autorité, l'affinité, et la prédiction[16].

Concernant leur fonctionnement, différents auteurs ont identifié trois étapes. La première est la collecte de données. Ces données sont issues d'informations explicites transmises consciemment (avis, réactions, notes, réponses à des enquêtes...), et d'informations implicites (clics, données comportementales, durée passée sur un site, historique…). La seconde étape correspond à l'analyse et la transformation des données collectées, afin d'appliquer un filtrage orienté vers l'utilisateur, ou le contenu en lui-même. La dernière étape est la fourniture de la recommandation à l'utilisateur[17].

Ces systèmes de recommandation ont permis une grande amélioration de la classification et de la recherche d'information, une véritable rationalisation des flux de trafic, et peuvent être considérés comme indispensables à l'utilisation efficace des moteurs de recherche notamment[18]. Aussi apparait-il évident qu'avec l'accroissement des données à disposition des GAFAM[19] (Google, Apple, Facebook, Amazon, Microsoft) et des autres grandes plateformes, les capacités de combinaison des données pertinentes d'utilisateurs et l'amélioration de l'intelligence artificielle (IA) de ces dernières leur fournissent des capacités de profilage – et par extension, de recommandations pertinentes – de plus en plus élevées.

---

[15] *Ibid*.
[16] CARDON (D.), *À quoi rêvent les algorithmes*, Ed. Seuil, 2015 p. 23.
[17] CASTAGNOS (S.), BRUN (A.), BOYER (A.), « La diversité : entre besoin et méfiance dans les systèmes de recommandation » *Revue I3 - Information Interaction Intelligence* [en ligne], Cépaduès, 2014, p. 3, [consulté le 24 juillet 2021].
[18] CONSEIL DE L'EUROPE, Comité consultatif de la convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, *Avis sur le projet de recommandation sur les impacts des systèmes algorithmiques sur les droits de l'Homme* [en ligne], Strasbourg, 21 novembre 2019, p. 11, [consulté le 25 juillet 2021].
[19] En 2017, 95% du marché de la données personnelles était détenu par les GAFAM : SEGOND (V.), « Des données personnelles très convoitées », *Le Monde* [en ligne], 28 mai 2017, [consulté le 29 juillet 2021].

Il est important de distinguer l'intelligence artificielle de l'algorithme, puisque si toute IA fait usage d'algorithmes, tous les algorithmes n'en sont pas un constitutif.

Après quelques discussions et évolutions sur ce que peut revêtir le concept d'intelligence artificielle, elle se définit de manière consensuelle comme « *l'ensemble des théories et techniques mises en œuvre en vue de réaliser des machines capables de simuler l'intelligence* »[20]. Si l'année 1956 a pu être habituellement fixée pour retenir la toute première apparition du terme « intelligence artificielle » lors de la conférence de Dartmouth[21], l'année 1950 peut aussi être considérée comme un point de départ historique pour l'intelligence artificielle. C'est à cette année qu'Alan Turing publia un article sur la question de savoir si une machine pouvait penser, article dans lequel fut introduit par la même occasion un test célèbre d'intelligence artificielle, dorénavant appelé *Test de Turing*[22]. Le progrès de l'intelligence artificielle a été ponctué de plusieurs périodes de progression et de financements en dents de scie, plus communément appelés « *hivers de l'IA* »[23] dans lesquels enthousiasme et pessimisme se sont alternés au sein de la communauté des chercheurs.

Ces périodes ont été accompagnées de deux approches techniques distinctes. La première approche, dite « *symbolique* ». Cette approche cognitive de l'IA représentée par John Mc Carthy et Marvin Minsky s'apparente à la création de mécanismes automatisés, par un enchainement d'instructions préétablies par un programmeur[24]. Ce sont des systèmes dont la logique est facilement explicable et démontrable. La seconde approche, le « *connexionnisme* », tend à préférer simuler les processus cognitifs du cerveau, afin de doter l'IA, en quelque sorte, d'un cerveau artificiel lui permettant d'apprendre par elle-même avec des connexions et liens établis par des exemples de son environnement plutôt que de règles établies[25]. Dans les années 1990, le « printemps » revient de nouveau et s'accompagne de réussites clés.

[20] Encyclopédie Larousse en ligne, *définition de l'intelligence artificielle* [en ligne], [consulté le 28 juillet 2021].
[21] LUC (J.), *L'intelligence artificielle n'existe pas*, Ed. First, 2019, p. 51.
[22] TURING (A. M.), « Computing Machinery and Intelligence », *Mind* [en ligne], vol. 59 n° 236, Octobre 2015, pp. 433-460, [consulté le 26 juillet 2021].
[23] D'ASCOLI (S.), *Comprendre la révolution de l'intelligence artificielle*, *op. cit*. note 12, p. 27.
[24] MENECEUR (Y.), *L'intelligence artificielle en procès : Plaidoyer pour une réglementation internationale et européenne*, Éd. Bruylant, 2020, p. 19.
[25] D'ASCOLI (S.), *Comprendre la révolution de l'intelligence artificielle*, *op. cit.* note 12, p. 26.

Un premier fracas médiatique est né en 1996 de la victoire aux échecs de Deep Blue, l'ordinateur d'IBM contre le champion du monde russe de l'époque Garry Kasparov[26]. Cependant, la victoire de l'ordinateur Deep Blue n'était pas réellement une révolution technique, il n'était qu'un *système expert*[27], un algorithme propre au connexionnisme qui excelle dans un domaine spécifique à l'aide de règles établies par l'humain, mais qui ne mettait pas en jeu un réel apprentissage.

La vraie révolution intervient à partir des années 2010 et marque un réel tournant vers le connexionnisme, avec notamment la victoire en 2012 de Geoffrey Hinton et ses étudiants lors du concours de reconnaissance d'image *ImageNet*[28], le triomphe en 2016 de l'algorithme *AlphaGo* de Google contre le champion du monde de go Lee Sedol[29] (le jeu de go étant bien plus complexe que les échecs en matière de possibilités de coups, et considéré jusqu'alors comme inatteignable pour un algorithme d'IA), ou encore la même année, l'expérience d'Alice et Bob, deux IA développées par Google qui ont réussi à chiffrer les messages envoyés entre elles afin de communiquer sans pouvoir être espionnées par une troisième IA[30].

Ces accomplissements ont en commun l'utilisation de l'apprentissage machine, plus communément appelé *Machine learning*. Le Journal officiel de la république française (JORF) s'est accordé sur une définition plutôt satisfaisante, en considérant l'apprentissage machine comme un « *processus par lequel un algorithme évalue et améliore ses performances sans l'intervention d'un programmeur, en répétant son exécution sur des jeux de données jusqu'à obtenir, de manière régulière, des résultats pertinents* »[31]. De nombreuses variantes techniques sont utilisées au sein du *Machine learning*, de telle sorte qu'il serait accessoire de toutes les

[26] BARTHELEMY (P.), « Garry Kasparov – Deep Blue : échec et bug », *Le monde* [en ligne], 21 juillet 2015, [consulté le 26 juillet 2021]

[27] V. en ce sens : ZARATE (P.), « L'intelligence artificielle d'hier à aujourd'hui », *Dalloz Droit Social*, 2 février 2021, p. 2. : *« Ces programmes ou logiciels capturent l'expertise d'un humain sur une tâche précise et grâce à un moteur d'inférence peuvent raisonner en activant certaines parties de la connaissance modélisées. La première étape lors de la réalisation de ces systèmes consiste à modéliser la connaissance des experts sous la forme de règles de production, par exemple de type « si condition alors action »* ».

[28] KRIZHEVSKY (A.), SUTSKEVER (I.), HINTON (G.), « ImageNet classification with deep convolutional neural networks », *NIPS'12 : Proceedings of the 25th International Conference on Neural Information Processing Systems* [en ligne], vol. 1, 3 décembre 2021, pp. 1091-1105, [consulté le 26 juillet 2021].

[29] LAUSSON (J.), « Jeu de go : victoire définitive 4 à 1 pour AlphaGo contre Lee Sedol », *Numerama* [en ligne], 15 mars 2016, [consulté le 27 juillet 2021].

[30] ABADI (M.), ANDERSEN (D. G.), « Learning to Protect Communications with Adversarial Neural Cryptography », *ArXiv* [en ligne], 24 octobre 2016, [consulté le 26 juillet 2021].

[31] « Vocabulaire de l'intelligence artificielle (liste de termes, expressions et définitions adoptées) », *JORF n°0285* [en ligne], texte n° 58, 9 décembre 2018, [consulté le 27 juillet 2021].

énumérer[32]. Une branche spécifique de l'apprentissage machine, nommée *Deep learning*, présentera un intérêt plus particulier, du fait de leur fonctionnement encore plus opaque que le *Machine learning* traditionnel, présentant déjà quant à lui de réels problèmes d'explicabilité des décisions prises[33].

Les derniers exploits en matière d'IA sont nombreux, et n'ont pas manqué de susciter plus de craintes et de fantasmes que ce que l'IA est réellement en capacité d'accomplir à ce jour. Un rapport d'information du Sénat énonçait à juste titre que « *les cycles d'espoirs et de déceptions qui jalonnent l'histoire de l'intelligence artificielle invitent à ne pas trop s'enthousiasmer en faisant preuve d'attentes irréalistes à l'égard des technologies existantes ou de celles mises à disposition dans un avenir proche.* »[34]. Ces propos ont été soutenus la même année par Isabelle Falque-Pierrotin, ancienne présidente de la CNIL, qui rappelait en guise d'introduction dans un rapport sur les enjeux éthiques des algorithmes et de l'IA que « *L'intelligence est le grand mythe de notre temps* », et que finalement, elle en « *dit sans doute plus de nos phantasmes et de nos angoisses que de ce que sera notre monde demain*. »[35].

Si l'intelligence artificielle se doit d'être démystifiée, les actions juridiques et techniques permettant d'éviter ses réels dangers ne doivent pas pour autant être écartées. Ce travail pluridisciplinaire est d'autant plus important lorsqu'il s'agit d'algorithmes pouvant être à l'origine d'une atteinte significative aux droits et libertés des individus. C'est la raison pour laquelle de nombreux rapports sur l'éthique de l'intelligence artificielle ont été produits ces dernières années afin de permettre la mise en place de grands principes, et qu'un projet de règlementation européenne sur l'intelligence artificielle a pu voir le jour en avril 2021[36].

Aujourd'hui, les systèmes de recommandation utilisés par les grandes plateformes en ligne utilisent pour la plupart ces solutions d'intelligence artificielle afin de faciliter la

[32] V. notamment pour plus de précisions sur la variété de modes d'apprentissages machine : CHAOUCHE (Y.), « Identifiez les différents types d'apprentissage automatiques », *formation Openclassrooms* [en ligne], mise à jour en 2021, [consulté le 27 juillet 2021].
[33] VILLANI (C.), *Donner un sens à l'intelligence artificielle : pour une stratégie nationale et européenne* [en ligne], rapport de mission parlementaire, 28 mars 2018, p. 141, [consulté le 27 juillet 2021].
[34] DE GANAY (C.), GILLOT (D.), *Pour une intelligence artificielle maîtrisée, utile et démystifiée* [en ligne], Sénat, rapport d'information n° 464, 15 mars 2017, [consulté le 27 juillet 2021].
[35] CNIL, *Comment permettre à l'Homme de garder la main ? : Les enjeux éthiques des algorithmes et de l'intelligence artificielle* [en ligne], rapport de décembre 2017, p. 4, [consulté le 26 juillet 2021].
[36] Proposition de Règlement du parlement européen et du Conseil établissant des règles harmonisées concernant l'intelligence artificielle (législation sur l'intelligence artificielle) et modifiant certains actes législatifs de l'Union, COM (2021) 206 final, 21 avril 2021.

recommandation du contenu pertinent pour les utilisateurs. La recommandation de contenu fait par ailleurs partie des utilisations les plus fréquentes et banalisées de l'intelligence artificielle[37]. Elle est en effet présente pour les moteurs de recherche, la recommandation de contenu culturel sur des plateformes telles que Netflix, le contenu affiché sur les réseaux sociaux, le choix publicitaire affiché, mais aussi pour la prospection électorale[38]. Dès lors, l'ensemble du contenu recommandé par ces algorithmes recouvre en réalité une grande variété de contenus et d'objectifs différents.

Du fait des différentes utilisations de ces systèmes de recommandation, leurs conséquences portent non seulement sur les utilisateurs confrontés à ces systèmes, mais également sur les entreprises et le marché de la concurrence lui-même.

## II - LES CONSEQUENCES INDUITES PAR L'UTILISATION DES SYSTEMES DE RECOMMANDATION

Malgré l'utilité avérée de ces algorithmes dans l'acheminement d'un contenu pertinent pour les utilisateurs, plusieurs questionnements et conséquences ont pu être relevés. Le fait de ne proposer qu'un certain type de contenu ne limiterait-il pas l'accès à l'information ? Qu'en est-il de la transparence dans les critères utilisés ? Les effets et conséquences ne sont pas les mêmes en fonction des plateformes utilisant ces techniques. Reprenant la même distinction que l'Observatoire européen de l'audiovisuel[39], une plateforme « *audiovisuelle et musicale* » comme Netflix, Spotify ou Deezer, ne soulève pas les mêmes enjeux en matière d'impact sur l'individu qu'un réseau social tel que Facebook, ou encore d'une plateforme de partage de vidéo telle que YouTube ou Dailymotion, qui héberge une variété beaucoup plus étendue de contenus culturels mais aussi politiques et commerciaux.

Cependant, l'un des effets que les systèmes de recommandation pourraient avoir a été conceptualisé sous l'appellation de *Bulle de filtre*, pour la première fois par Eli Pariser, activiste

[37] CNIL, *Comment permettre à l'Homme de garder la main ? : Les enjeux éthiques des algorithmes et de l'intelligence artificielle*, *op. cit.* note 35, p. 21.
[38] *Ibid.*
[39] CABRERA BLAZQUEZ (F. J.), CAPPELLO (M.), RABIE (I.) et al., *Le cadre juridique relatif aux plateformes de partage de vidéos* [en ligne] , IRIS Plus, Observatoire européen de l'audiovisuel, Strasbourg, 2018, p. 7, [consulté le 26 juillet 2021].

pour un internet au service de la société, et auteur du livre intitulé *The Filter Bubble*[40], qui présente ce concept et ses effets. Selon Eli Pariser, l'utilisation surabondante d'algorithmes jouant un rôle dans le classement et la recommandation de contenu aurait un effet de nuisance dans la pluralité de contenus recommandés, qu'ils aient une vocation commerciale, culturelle ou politique. De ce fait, en filtrant les informations par le biais d'algorithmes s'appuyant sur les caractéristiques du profil de l'utilisateur, ces algorithmes augmenteraient la propension des individus à ne consulter que du contenu conforme à leurs préférences, préférences étant bien entendu estimées en fonction des données d'activités collectées sur ces individus. En matière de recommandations, le sociologique Dominique Cardon a pu souligner en 2017 que malgré la diversité informationnelle apportée par le numérique, certains dangers étaient à soulever : *« des gens curieux vont envoyer des signaux de curiosité et vont se voir incités en retour à la curiosité. En revanche, des gens donnant peu de traces de curiosité vont être dirigés vers moins de diversité* »[41].

L'usage des algorithmes de recommandation faciliterait aussi la création de *chambres d'écho*, c'est-à-dire la répétition d'une seule idée et position formant un « écho » médiatique sur un sujet donné, qui a pour effet de conforter les utilisateurs dans leurs certitudes et convictions sur le plan individuel[42], mais aussi d'augmenter l'effet de polarisation des débats sur le plan collectif[43]. Ce concept, proche de la *bulle de filtre***,** se distingue principalement du fait que la chambre d'écho est créée par les utilisateurs eux-mêmes, tandis que la bulle de filtre est formée par les algorithmes[44]. Les chambres d'écho ne dépendent donc pas uniquement du numérique et peuvent se retrouver dans une diffusion plus traditionnelle de l'information, mais son effet serait justement amplifié par le modèle de recommandation constitué par les algorithmes[45].

[40] PARISER (E.), *The filter bubble: What The Internet Is Hiding From You,* Ed. Penguin Group, 2011, 304 p.
[41] CARDON (D.), « Évènement de lancement du cycle de débats publics sur les enjeux éthiques des algorithmes », *CNIL* [en ligne], 23 janvier 2017, p.9, [consulté le 28 juillet 2021].
[42] LESAGE (N.), « Des universitaires vont étudier les chambres d'écho responsables de la toxicité de Twitter », *Numerama* [en ligne], 31 juillet 2018, [consulté le 28 juillet 2021].
[43] BARBERA (P.), JOST (J.T.), NAGLER (J.) et al., « Tweeting From Left to Right: Is online Political Communication More Than an Echo Chamber? », *Psychological Science* [en ligne], Vol. 26 n° 10 (2015) : 1531-42, Octobre 2015, p. 2, [consulté le 28 juillet 2021].
[44] SUMPTER (D.), *Outnumbered : From Facebook and Google to fake news and filter-bubbles – the algorithms that control our lives*, Blommsbury Publishing, 2018, p. 186.
[45] GESCHKE (D.), LORENZ (J.), HOLTZ (P.), « The triple-filter bubble: Using agent-based modelling to test a meta-theoretical framework for the emergence of filter bubbles and echo chambers », *British Journal of Social Psychology* [en ligne], vol. 58 n° 1, pp. 129-149, [consulté le 1 aout 2021].

Les chambres d'écho et bulles de filtre sont liées à certains biais cognitifs décrits en psychologie, le plus pertinent pour ces effets étant le *biais de confirmation*[46]. Il s'agit d'un biais cognitif décrivant une tendance à rechercher de l'information qui confirme des croyances établies, tout en ne prenant pas en compte les opinions contradictoires afin d'éviter une *dissonance cognitive*, un inconfort psychologique généré par l'incohérence entre les préférences et croyances d'un individu, et une information ou situation contradictoire à celles-ci[47].

Ainsi, de nombreuses études ont été réalisées afin de mesurer ces effets. Le consensus n'a pas été atteint concernant l'impact de ces effets sur les individus. Alors que certaines études soulignent leur impact tant sur la polarisation de la société, mais aussi à recommander aux utilisateurs du contenu de plus en plus extrême[48], d'autres, tout en admettant la réalité de ces effets, ont tenté de les nuancer. Tel était le cas notamment d'une étude faite par l'équipe scientifique de Facebook en 2015, concluant que malgré la réalité avérée de ces effets, elle n'était pas aussi importante que ce que l'état de l'Art le pensait[49]. Cependant, plusieurs sociologues[50] et Eli Pariser[51] ont critiqué la pertinence de cette étude par le manque de représentativité de l'échantillon, la difficulté de clairement faire une moyenne de techniques changeant constamment, et surtout, l'absence de reproductibilité de l'expérience par des chercheurs indépendants n'appartenant pas à Facebook. Conscient de l'importance grandissante de ces algorithmes, d'autres groupes de chercheurs ont effectué des recherches sur d'autres plateformes.

En 2019 par exemple, YouTube a été « audité » par un groupe de chercheurs, dont le travail consistait notamment à examiner si l'algorithme de recommandation de YouTube avait tendance à diriger les utilisateurs vers du contenu de plus en plus extrême (et par extension, du

---

[46] BRONNER (G.), *La démocratie des crédules*, Puf, 2013, p. 49. Bronner précisait notamment que : « *Le biais de confirmation permet donc d'affermir toutes sortes de croyances, les plus anodines, (…) comme les plus spectaculaires.* ».

[47] ROUAULT (M.), « Chapitre IX. Décision et apprentissage », dans : COLLINS (T.), *La cognition. Du neurone à la société* [en ligne], Gallimard, Folio Essais, 2018, pp. 371-419, [consulté le 1 août 2021].

[48] V. notamment : GESCHKE (D.), « The triple-filter bubble: Using agent-based modelling to test a meta-theoretical framework for the emergence of filter bubbles and echo chambers », *op. cit.*

[49] BAKSHY (E.), MESSING (S.), ADAMIC (L.), « Exposure to ideologically diverse news and opinion on Facebook », *Sciences* [en ligne], vol. 348 n° 6239, 5 juin 2015, pp. 1130-1132, [consulté le 1 aout 2021].

[50] LUMB (D.), « Why Scientists Are Upset About The Facebook Filter Bubble Study », *Fastcompany* [en ligne], 5 août 2015, [consulté le 1 aout 2021].

[51] PARISER (E.), « Did Facebook's Big Study Kill My Filter Bubble Thesis? Not really — and here's why », *Wired* [en ligne], 5 juillet 2015, [consulté le 1 août 2021].

contenu politiquement radicalisant)[52]. L'analyse a été effectuée sur plus de 2 millions de recommandations effectuées par l'algorithme, ainsi que sur les vidéos et commentaires publiés. Il a été conclu – avec les réserves propres aux limitations techniques de la démonstration – que cette tendance concordait avec les différents récits et témoignages médiatiques ayant été faits au sujet de l'algorithme de YouTube[53], et que la démonstration fournissait une preuve solide de la tendance des recommandations de YouTube à suggérer du contenu toujours plus extrême.

Cette présentation non exhaustive des différents débats sur l'impact de ces systèmes semble depuis quelques temps converger vers une réalité perçue par tous. Le Conseil de l'Europe affirme depuis 2017 que la recherche universitaire a révélé la mesure dans laquelle la manipulation et l'organisation du contenu recommandé sur les plateformes pouvait faire « *basculer* » un vote[54]. Ce dernier a ajouté qu'il a été montré que les élections pouvaient être remportées par les candidats disposant des meilleurs outils technologiques servant à manipuler les électeurs, en jouant parfois sur l'affectif et l'irrationnel[55]. C'est un fait pouvant compromettre le droit à des élections libres, et plus largement le modèle démocratique actuel.

L'état actuel des garanties réglementaires ne semble pas encore satisfaire le principe de précaution à ce sujet. Ce principe était avancé par le Conseil de l'Europe en 2020 concernant l'impact des systèmes algorithmiques[56], et entre autres, les algorithmes créés pour une fonction de « *classification et de recherche des informations numériques* »[57]. Ce principe de précaution se traduit selon le Conseil de l'Europe par la prise de mesures permettant d'amplifier les effets positifs dus à l'usage des algorithmes, tout en diminuant les éventuels effets négatifs. Ce principe initialement prévu par la loi Barnier[58] et consacré constitutionnellement depuis 2005[59], est un principe selon lequel « *l'absence de certitudes, compte tenu des connaissances scientifiques et techniques du moment, ne doit pas retarder l'adoption de mesures effectives et*

[52] HORTA RIBEIRO (M.), OTTONI (R.), WEST (R.), et al., « Auditing Radicalization Pathways on YouTube », *Computers and Society* [en ligne], 22 août 2019, [consulté le 2 août 2021].
[53] SIX (N.), « L'algorithme de recommandation de YouTube critiqué pour sa mise en avant de contenus extrêmes », *Le monde* [en ligne], 16 octobre 2019, [consulté le 2 août 2021].
[54] CONSEIL DE L'EUROPE, *Algorithmes et droits humains* [en ligne], étude du Conseil de l'Europe DGI (2017) 12, 2017, p. 33, [consulté le 29 juillet 2021].
[55] *Ibid.*
[56] CONSEIL DE L'EUROPE, *Recommandation CM/Rec(2020)1 du Comité des Ministres aux États membres sur les impacts des systèmes algorithmiques sur les droits de l'homme* [en ligne], 8 avril 2020, point A. 15, [consulté le 29 juillet 2021].
[57] *Ibid.*, point A. 3.
[58] Loi n° 95-101 du 2 février 1995 relative au renforcement de la protection de l'environnement.
[59] Loi constitutionnelle n° 2005-205 du 1er mars 2005 relative à la Charte de l'environnement.

*proportionnées visant à prévenir un risque …* »[60]. Initialement prévu pour le domaine environnemental, ce principe a été étendu à d'autres domaines tels que la santé publique, la sécurité alimentaire, et les innovations technologiques en général[61].

Par leurs nombreuses conséquences, les algorithmes de recommandation et plus généralement le contenu recommandé en ligne, ont pu susciter l'intérêt de nombreux acteurs et organes institutionnels.

## III - UN INTERET MANIFESTE POUR LES SYSTEMES DE RECOMMANDATION

L'influence exercée par ce mode de diffusion du contenu en ligne a suscité de plus en plus d'intérêt de la part de nombreux acteurs. En effet, si les révélations de l'affaire Snowden de 2013 ont été un moteur supplémentaire vers la mise en place du RGPD[62], le scandale de Cambridge Analytica de 2018 se trouve être une affaire mettant en lumière les possibles dérives de ces systèmes algorithmiques, et des possibilités d'influence suite à l'analyse comportementale des individus. Lors des élections américaines, cette société a utilisé les données personnelles de plus de 87 millions d'utilisateurs américains recueillies sur Facebook afin d'établir un profil *psychographique*[63] de ces derniers et une analyse de leur comportement. Parmi ces données, y figuraient sans surprise des données liées aux opinions politiques et origines ethniques des individus. Ainsi, les profils considérés comme des utilisateurs *« influencable*s », sans position politique définie, étaient dès lors envahis de contenu publicitaire ciblé et de fausses informations afin d'influencer les élections de 2016 en faveur de Donald Trump[64]. Le même type de procédé a été utilisé lors du vote sur le Brexit[65].

[60] Code de l'environnement, art. L110-1.
[61] LARRERE (C.), « Le principe de précaution et ses critiques », *Innovations* [en ligne], vol. n° 18, n°. 2, 2003, pp. 9-26, [consulté le 29 juillet 2021].
[62] GOYA (C.), « Cédric Villani dit que le RGPD n'aurait pas pu naître sans 'l'héroïsme' du lanceur d'alerte Edward Snowden », *Business insider* [en ligne], 14 juin 2018, [consulté le 1 août 2021].
[63] V. pour plus de précisions : « *La segmentation psychographique cherche à comprendre les valeurs, les intérêts et les modes de vie des individus afin de découvrir leurs besoins et motivations* », HARDCASTLE (S.), HAGGER (M.), « Psychographic Profiling for Effective Health Behavior Change Interventions », *Health Psychologu and Behavioural Medicine Research Group* [en ligne], Université de Curtin, 6 janvier 2016, [consulté le 27 juillet 2021].
[64] LEWIS (P.), HILDER (P.), « Leaked: Cambridge Analytica's blueprint for Trump victory », *The Guardian* [en ligne], 23 mars 2018, [consulté le 28 juillet 2021].
[65] HERN (A.), « Cambridge Analytica did work for Leave.EU, emails confirm », *The Guardian* [en ligne], 30 juillet 2019, [consulté le 28 juillet 2021].

De ce fait, de nombreux acteurs, organes nationaux et européens appellent à l'éclaircissement de ces usages, et à la mise en place de nouvelles mesures pour encadrer ces systèmes.

Sur le plan éthique, la CNIL évoquait déjà en 2017 dans son rapport *Comment permettre à l'Homme de garder la main,* propos des questions éthiques à régler, que « *Les algorithmes de recommandation, s'ils ne constituent techniquement qu'une fraction des différents types d'algorithmes, constituent une partie importante de la question* »[66].

Margrethe Vestager, vice-présidente exécutive de la Commission européenne, évoquait à l'occasion d'un discours en présence de l'ONG AlgorithmWatch en octobre 2020 la problématique des algorithmes de recommandation. Ces algorithmes qui font le succès énorme de ces plateformes « *peuvent aussi avoir de graves effets sur la santé de nos démocraties* »[67]. La commissaire européenne soulignait notamment le problème de transparence de ces derniers, puisque si le fait que les informations soient filtrées n'est pas nouveau, « *lorsque ces choix sont faits par des algorithmes, il peut être difficile de comprendre comment ils ont pris leurs décisions* »[68].

Le Conseil supérieur de l'audiovisuel (CSA) s'est aussi intéressé à la question de la « *responsabilité des plateformes de partage de contenus* » et sur « *l'effet de l'algorithme de recommandation* »[69], notamment dans une étude menée en 2019 sur la plateforme YouTube, dans laquelle le CSA a pu montrer le très grand impact des recommandations sur le visionnage de contenu. Dans cette étude, 86% des participants estimaient que le contenu recommandé était souvent semblable, et surtout, que 70% de participants suivent les recommandations de contenu[70]. Il ressort de l'étude du CSA que « *La recommandation algorithmique pourrait produire des phénomènes dits de chambre d'écho à l'échelle du groupe de participants pouvant affecter la diversité des contenus proposés et le pluralisme des opinions exprimées dans les vidéos recommandées* »[71]. Par ailleurs, les chiffres de cette étude corroborent parfaitement ceux

[66] CNIL, *Comment permettre à l'Homme de garder la main ? : Les enjeux éthiques des algorithmes et de l'intelligence artificielle*, *op. cit.* note 35, p. 19.
[67] VESTAGER (M.), *Algorithms and democracy* [en ligne], AlgorithmWatch Online Policy Dialogue, 30 octobre 2020, [consulté le 2 aout 2021].
[68] *Ibid*.
[69] CSA, *Capacité à informer des algorithmes de recommandation : Une expérience sur le service Youtube*, *op. cit.* note 4, p. 64.
[70] *Ibid*., p. 28.
[71] *Ibid*., p. 5.

donnés par l'un des dirigeants de YouTube, Neal Mohan, estimant en 2018 que 70% du contenu total visionné sur YouTube, était du contenu issu de ces systèmes[72].

Enfin, le Comité européen de la protection des données (CEPD), a lui aussi rendu un avis en 2018 alertant sur les problématiques économiques et sociales induites par la segmentation des individus, la recommandation de contenu et la publicité ciblée, toutes deux basées sur le profilage. Le CEPD évoquait à ce titre que l'environnement en ligne personnalisé et microciblé avait pour conséquence de créer « des « bulle de filtrage » au sein desquelles les gens sont toujours exposés au même type d'informations et confrontés à moins d'opinions, d'où une polarisation politique et idéologique accrue »[73].

Il serait trop facile de tenir les algorithmes pour seuls responsables de tous les maux. Des implications ici bien humaines étaient à l'origine des recommandations de contenu pour les profils « *influençable*s » lors du scandale Cambridge Analytica. De même, il est dans la nature humaine d'être soumis à ses propres biais cognitifs et de tenter de résoudre les dissonances cognitives auxquelles l'individu doit faire face. C'est donc un chantier très complexe pour les différents acteurs, juridiques, comme techniques ou sociologiques, qui tenteraient d'appréhender et de résoudre ces problématiques.

## IV - PROBLEMATIQUE, METHODE DE RESOLUTION ET PLAN

Si certains effets indésirables des systèmes de recommandations se sont vus attribuer des garanties juridiques notamment les problèmes liés à la diffusion de fausses informations, ou en matière de transparence, d'autres points concernant les bulles de filtres ou chambres d'écho n'ont donc à ce jour pas eu de réponse juridique satisfaisante. De même, si les disciplines scientifiques et sociologiques, ainsi que de nombreux acteurs de la sphère juridique manifestent un intérêt sur les conséquences de ces systèmes et la régulation du contenu recommandé, il a été constaté lors de la phase de recherche que peu d'articles juridiques cherchant à connecter le droit à la problématique des systèmes de recommandation en particulier avaient été publiés à

[72] SIX (N.), « L'algorithme de recommandation de YouTube critiqué pour sa mise en avant de contenus extrêmes », *op.cit.* note 53.
[73] CEPD, *Avis du CEPD sur la manipulation en ligne et les données à caractère personnel* [en ligne], avis n° 3/2018, 19 mars 2018, p. 8, [consulté le 1 août 2021].

ce jour. Pourtant, s'il existe bien une discipline permettant d'harmoniser les pratiques techniques et réguler un comportement préjudiciable pour la société, il s'agit bien du Droit.

Tout l'enjeu de ce mémoire est donc de s'interroger sur les garanties juridiques permettant de réguler la recommandation du contenu, de mettre en relief leurs faiblesses actuelles et d'envisager de nouveaux outils permettant une véritable régulation des systèmes de recommandation en accord avec les principes du droit déjà existants. En d'autres termes, ce mémoire s'attache à étudier dans quelle mesure les systèmes de recommandations peuvent être encadrés ; ainsi qu'à interroger les problèmes actuels issus de la recommandation du contenu, tout en présentant de nouvelles idées juridiques et techniques pouvant potentiellement s'appliquer à ces systèmes dans un futur proche.

Les analyses présentes au sein de ce travail se limiteront aux systèmes de recommandation utilisés par les grandes plateformes, ainsi que sur les impacts d'une recommandation du contenu pour les utilisateurs. Par conséquent, ce mémoire ne traitera pas des systèmes algorithmiques d'aide à la décision, notamment ceux utilisés dans les domaines de la justice, de la police, de l'administration ou de la médecine. En effet, bien que ces algorithmes puissent avoir une fonction de recommandation vers la prise d'une décision, voir fonction de prise de décision automatisée, leur étude fait déjà l'objet d'une longue littérature juridique, et ils ne sont pas destinés à la même finalité que les algorithmes de recommandation de contenu utilisés dans le secteur privé.

De la même manière, cette étude des systèmes de recommandation se concentra davantage sur les impacts en matière de droits et libertés des individus, et non sur les systèmes de recommandation utilisés dans le domaine culturel. Bien que le fonctionnement de ces algorithmes soit similaire, ils ne soulèvent pas les mêmes enjeux juridiques, et mériteraient une recherche entièrement consacrée à leur étude.

Ce faisant, la présente recherche soulignera l'impact des systèmes de recommandation contemporains sur les droits et libertés des individus, et la carence juridique dont ces systèmes font l'objet (Partie I). Cette partie de la recherche étudiera plus en profondeur l'état actuel du profilage et de ses conséquences, ainsi que la logique de recommandation mise en place par les plateformes, fonctionnant principalement pour servir l'économie de l'attention, et pouvant porter un préjudice individuel et collectif encore peu souvent présenté. Enfin, une étude de

l’efficacité des réponses juridiques apportées par le législateur en matière de circulation des fausses informations, mais aussi de la réglementation actuelle sur la protection des données, et plus spécifiquement sur le profilage sera effectuée, en soulignant l’insuffisance de ces réponses face au contexte actuel.

L’étude de l’impact du contenu recommandé et de la réponse juridique à celui-ci s’accompagnera d’une analyse des réglementations à venir en matière de législation sur les services numériques, ainsi que sur les améliorations envisagées de cette règlementation par différents acteurs. Enfin de potentielles mesures juridiques et techniques, pouvant s’appliquer plus spécifiquement aux systèmes de recommandation seront proposées (Partie II). En effet, les prochains apports en matière de transparence et de contrôle des systèmes de recommandation peuvent inspirer la mise en place de nouveaux droits transversaux propres à encadrer ces effets, et nourrissent l’espoir d’une véritable responsabilisation des plateformes mettant en place ces solutions.

# PREMIERE PARTIE – UN ENCADREMENT LACUNAIRE DES SYSTEMES DE RECOMMANDATION

Il convient en premier lieu d'écarter une potentielle idée reçue. Les algorithmes font-ils l'objet d'un vide juridique actuellement ? De la même manière qu'il n'existe pas de véritable vide juridique – excepté au parc national de Yellowstone[74] –, les algorithmes étaient déjà encadrés par de grands principes issus de la Loi Informatique et Libertés[75] (LIL), datant maintenant de 43 ans. Le paléolithique à l'échelle de la technologie. En effet, trois principes sont contenus dans cette loi, qui se rattachent au principe général déjà contenu en son premier article : « *L'informatique doit être au service de chaque citoyen. Son développement doit s'opérer dans le cadre de la coopération internationale. 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* »[76]. Selon Sonia Desmoulin-Canselier et Daniel le Métayer, ce premier texte, qui a pour finalité de protéger les individus contre un traitement illégitime de leurs données personnelles, illustre surtout une volonté de tirer le meilleur parti des progrès techniques tout en garantissant le respect des libertés et des droits fondamentaux[77].

Selon le rapport de la CNIL sur l'intelligence artificielle[78], de ce principe général découlent trois autres principes applicables aux algorithmes, qui ont ainsi une portée européenne par la mise en place du RGPD en 2018.

Premièrement l'utilisation des données nécessaires au fonctionnement de ces algorithmes est encadrée par les principes de la protection des données, notamment les principes de licéité, de finalité, de sécurité, ou encore de limitation de la durée de conservation[79]. Cette utilisation laisse aussi la possibilité aux personnes concernées par le traitement d'exercer leurs droits[80].

[74] KALT (B.), « The Perfect Crime », *Georgetown Law Journal* [en ligne], vol. 93, 2005, pp. 675-688, [consulté le 1 août 2021].
[75] Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.
[76] *Ibid*., art. 1.
[77] DESMOULIN-CANSELIER (S.), LE METAYER (D.), *Décider avec les algorithmes : Quelle place pour l'Homme, quelle place pour le droit ?* Dalloz, 2020, p. 109.
[78] CNIL, « Comment permettre à l'Homme de garder la main ? : Les enjeux éthiques des algorithmes et de l'intelligence artificielle », *op. cit.* note 35, p. 45.
[79] RGPD, art. 5.1.
[80] *Ibid.*, art. 12 à 22.

Deuxièmement, il est interdit pour un algorithme de prendre des décisions seul, sans intervention humaine, et qui pourrait avoir des conséquences graves pour les droits et libertés des personnes[81]. Enfin, les personnes concernées par un traitement algorithmique ont un droit d'obtenir auprès du responsable de traitement des informations sur la logique de fonctionnement de l'algorithme[82].

Cette logique d'information a par ailleurs été renforcée pour l'administration depuis la loi pour une République numérique de 2016. Celle-ci, dans une optique d'*Open data* (ouverture des données)[83], a inséré un article dans le Code des relations entre le public et l'administration (CRPA) prévoyant pour les administrations faisant usage de traitements algorithmiques de mettre à disposition leur code source pour les algorithmes utilisés par l'administration et d'autre part, les règles fondant la décision de l'algorithme[84]. Au-delà de l'encadrement des algorithmes, les plateformes elles-mêmes bénéficient de divers encadrements fragmentés dans plusieurs législations et codes. Le Code de la consommation par exemple, a mis en place une obligation d'information sur le fonctionnement des services des opérateurs de plateforme en ligne reposant sur « *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 (…)* »[85].

Si ces principes sont d'ores et déjà existants, sont-ils pour autant respectés concernant les algorithmes de recommandation ? Pour répondre à cette interrogation, il sera nécessaire de comprendre en premier lieu la raison pour laquelle ces systèmes, en étant au service de l'économie de l'attention, causent une réelle atteinte aux droits des individus (Chapitre 1). De cette atteinte, il sera vu que certaines protections prévues en cas d'utilisation préjudiciable de ces systèmes se révèlent insuffisantes pour protéger les individus des systèmes de recommandation (Chapitre 2).

[81] LIL, art. 10, et RGPD, art. 22.
[82] LIL, art. 39, et RGPD, art. 15.1.h.
[83] V. en ce sens : CONSEIL NATIONAL DU NUMERIQUE, *Avis n°2015-3 relatif au projet de loi pour une République numérique* [en ligne], 30 novembre 2015, p. 3, [consulté le 2 aout 2021], L'open data se définit comme la mise à « *disposition des citoyens, des acteurs de la société civile et de l'économie, les données produites, collectées ou détenues dans le cadre d'une mission de service public et d'en autoriser la réutilisation à des fins privées ou commerciales* ».
[84] CRPA, art. L. 312-1-3.
[85] C. consomm., art. L. 111-7, I, 1°.

# CHAPITRE 1 – DES SYSTEMES DE RECOMMANDATION AU SERVICE DE L'ECONOMIE DE L'ATTENTION

La part des investissements dans la publicité en ligne augmente de plus en plus chaque année. En France, 2016 a été l'année durant laquelle l'investissement publicitaire sur internet dépassait pour la première fois celui de la télévision[86]. Ce basculement de la publicité vers internet a une explication simple. Là où la publicité par télévision était générale et adressée à des auditeurs anonymes, la publicité sur internet s'accompagne d'outils de ciblage marketing permettant de proposer des produits aux internautes les plus susceptibles d'être intéressés.

Une autre raison de ce basculement est l'utilisation de nombreux outils par les plateformes afin de capter au maximum l'attention des internautes. C'est un cercle vertueux pour les deux parties : les publicitaires et autres annonceurs ciblent mieux et plus efficacement les individus, tandis que les plateformes augmentent leurs rémunérations du fait de l'intérêt que les annonceurs (publicitaires ou non) leur portent.

Cette logique appartient à ce qui est communément appelé *l'économie de l'attention*. Ce concept décrivant une économie dont l'attention des consommateurs serait la première rareté et la plus précieuse source de valeur[87], était déjà décrite par Simon Herbert en 1969, bien avant l'usage des techniques de pointes utilisées par les plateformes. Herbert expliquait ce concept de la manière suivante : « *Dans un monde riche en informations, l'abondance d'informations entraîne la pénurie d'une autre ressource : la rareté devient ce que consomme l'information. Ce que l'information consomme est assez évident : c'est l'attention de ses receveurs. Donc une abondance d'informations crée une rareté de l'attention et le besoin de répartir efficacement cette attention parmi la surabondance des sources d'informations qui peuvent la consommer* »[88]. C'est par ce principe d'*économie de l'attention* (la finalité), combiné aux sciences cognitives (la méthode), et à l'usage d'algorithmes (l'instrument), que les grandes plateformes détiennent toutes les clés de l'attention de l'utilisateur (le sujet). Ainsi, Facebook

[86] GOLA (R.) « Publicité digitale et encadrement des algorithmes », *RLDI*, n° 141, octobre 2017.
[87] CITTON (Y.), « Introduction », dans : CITTON (Y.), *L'économie de l'attention. Nouvel horizon du capitalisme ?* [en ligne], La Découverte, 2014, pp. 7-31, [consulté le 5 août 2021].
[88] HERBERT (S.), « Designing Organizations for an Information-Rich World », Dans : GREENBERGER (M.), « Computers, communications, and the public interest », *The John Hopkins Press* [en ligne], 1971, pp. 38-72. [Consulté le 5 août 2021].

peut exercer une influence sur le ressenti de l'humain par un effet de contagion émotionnelle, en modifiant l'ordre du contenu recommandé par son algorithme de recommandation, le *News Feed Algorithm*[89].

Les différentes thèses de l'économie de l'attention cherchent aussi à expliquer les différentes techniques permettant d'optimiser les effets de la publicité ciblée. Certaines techniques comme *l'infinite scrolling*, consistant à réactualiser indéfiniment le fil d'actualité d'un réseau social, ou *l'autoplay*, présent sur Youtube et Netflix afin de garder au maximum l'individu captif de la plateforme, sont deux pratiques expliquées dans le documentaire *The social Dilemma* disponible sur… Netflix.

Le rôle du profilage est tout aussi important au sein de cette *économie de l'attention*, puisque les plateformes en ligne ont pour objectif préalable d'accumuler un maximum d'informations comportementales sur l'individu, afin d'optimiser l'efficacité des systèmes de recommandation. Cette pratique explique en somme la présence aussi importante de bulles de filtres et de chambres d'écho, dans lesquelles la diffusion de certains messages et contenus est amplifiée[90].

Il sera vu dans un premier temps les différentes pratiques en rapport avec les systèmes de recommandation, permettant aux plateformes de maximiser leurs intérêts par ces outils technologiques (Section 1). Ainsi, il sera pertinent de constater dans quelle mesure ces différents usages portent atteinte aux droits et libertés des individus, ainsi qu'au marché en lui-même (Section 2).

[89] « Des utilisateurs de Facebook « manipulés » pour une expérience psychologique », *Le monde* [en ligne] , 30 juin 2014, [consulté le 1 août 2021].
[90] POULLET (Y.), RUFFO DE CALABRE (M.-N.), « La régulation des réseaux sociaux », *Études* [en ligne], vol. n° 6, 2021, *pp*. 19-30, [consulté le 1 août 2021].

## SECTION 1 – LES DIFFERENTS USAGES GRAVITANT AUTOUR DE LA RECOMMANDATION DE CONTENUS

Schématiquement, la recommandation du contenu d'une plateforme suit la logique d'une phase de collecte des données pertinentes, suivie par l'exploitation de ces données sous la forme d'un profilage de l'utilisateur visé, permettant de déduire quel contenu est le plus susceptible d'être apprécié par ce dernier. Constituant ainsi la dernière phase, la recommandation s'attache à distribuer le contenu sélectionné avec soin par l'algorithme, vers l'utilisateur de la plateforme.

Ces systèmes n'incluent pas uniquement la recommandation de contenu dans le sens de ce qui est imaginable pour les publications sur les réseaux sociaux, ou sur les plateformes de partage de contenu. Il est aussi question du référencement d'articles sur des plateformes comme Amazon, ou encore de la classification des résultats de recherches sur des moteurs de recherche comme ceux de Google.

Avant toute chose, il apparait donc intéressant de voir les pratiques ayant un impact direct sur les individus utilisateurs des services accordés par les grandes plateformes, et dans un second temps, les pratiques qui, en plus d'avoir un impact sur les utilisateurs, affectent d'autant plus le marché de la concurrence. Plus précisément, il sera question d'analyser les pratiques de profilage et de microciblage permettant de contrôler les recommandations faites aux individus (I), et enfin, de constater que certaines pratiques anticoncurrentielles trouvent leurs sources dans la manipulation des recommandations (II).

### I - Du profilage au microciblage : caractérisation d'une pratique préjudiciable pour les individus

Le RGPD a apporté une définition, plutôt large, du processus de profilage. Ce dernier est considéré comme « *toute forme de traitement automatisé de données à caractère personnel consistant à utiliser ces données à caractère personnel pour évaluer certains aspects personnels relatifs à une personne physique, notamment pour analyser ou prédire des éléments concernant le rendement au travail, la situation économique, la santé, les préférences*

*personnelles, les intérêts, la fiabilité, le comportement, la localisation ou les déplacements de cette personne physique* »[91].

Ce sont essentiellement les techniques de *machine learning*, et surtout de *deep learning* qui ont permis un développement aussi drastique des techniques de profilage.

Comme l'affirmait le rapport *Donner un sens à l'intelligence artificielle* de Cédric Villani en 2018, la collecte de données est généralement le point de départ nécessaire à toute utilisation d'algorithmes d'intelligence artificielle[92]. Les différents modèles de systèmes de recommandation utilisés par les différentes plateformes ne font pas exception à cette règle. Ces algorithmes puisent dans les ressources disponibles en *Open source*[93], et dans des bases de données nommées *dataset* afin d'entrainer leurs algorithmes. Lors de la conception d'un système de profilage, la plupart des plateformes doivent opérer un choix entre la transparence de l'algorithme, et sa précision. De manière générale, un modèle constitué de règles plutôt simples sera plus facilement transparent, et inversement[94].

Une fois que le système est en activité, le profilage des utilisateurs s'effectue grâce à la collecte des traces de navigation, qui permettent à l'algorithme d'établir une prédiction constante sur son intérêt pour une annonce, ou un contenu en particulier. Cela permet, entre autres, d'évaluer en temps réel une valeur déterminée pour un espace publicitaire présent sur la page consultée[95], ainsi que l'intérêt porté sur un contenu ou produit recommandé dans le cas des plateformes de partage de contenu telles que YouTube.

Ce profilage, puisqu'il est automatisé, permet à l'algorithme de repérer des motifs et caractéristiques que l'être humain ne peut pas – ou difficilement – repérer par lui-même. Certaines techniques peuvent en effet être très pointues, comme par exemple, l'analyse de l'état

---

[91] RGPD, art. 4.4.
[92] VILLANI (C.), *Donner un sens à l'intelligence artificielle : pour une stratégie nationale et européenne, op. cit.*, p. 14.
[93] V. notamment : OFFICE QUEBECOIS DE LA LANGUE FRANÇAISE, « Code source libre », *Grand dictionnaire terminologique* [en ligne], [consulté le 5 août 2021]. L'Open source, ou *« Code source libre »*, se définit comme un *« Code source que l'on rend disponible gratuitement pour qu'il puisse être modifié et redistribué, dans un contexte de développement communautaire*. ».
[94] POUILLET (Y.), FRENAY (B.), *Comité consultatif de la convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel* [en ligne], rapport du Conseil de l'Europe, T-PD(2019)07, Strasbourg, 9 septembre 2019, p. 16, [consulté le 2 août 2021].
[95] GOLA (R.) « Publicité digitale et encadrement des algorithmes », *RLDI*, n° 141, octobre 2017.

de nervosité ou de fatigue d'une personne en fonction de la façon dont elle tape sur le clavier[96], ou encore la prédiction du profil socio-économique d'une personne en fonction de la collecte de certaines informations telles que la localisation, le répertoire d'appel et les contacts[97].

Les performances du profilage ont été décuplées par les nouvelles possibilités d'exploitation de données de ces dernières années. À titre d'exemple, une plateforme telle que Facebook collecte plus de 52 000 caractéristiques personnelles différentes afin de trier et classer ses utilisateurs, en analysant les messages, *likes*, partages, cercles d'amis, et beaucoup d'autres données comportementales[98]. La plupart de ces plateformes n'utilisent pas uniquement leurs propres bases de données afin d'effectuer ce type de profilage très précis, mais font aussi appel à des courtiers en données, ou « *Data broker* », qui cherchent à collecter des données en masse sur internet, dans l'objectif de les commercialiser et de les revendre à d'autres entreprises[99]. Dès 2013, Facebook a démarré un partenariat avec plusieurs *databrokers* afin d'améliorer ses capacités de profilage des individus[100].

Par son perfectionnement technique et son usage intrusif, le profilage est sujet, de manière générale, à de nombreux débats éthiques. À ce titre, la CNIL a pu identifier plusieurs grandes problématiques éthiques induites par l'utilisation des algorithmes d'intelligence artificielle. Parmi elles figurent le profilage et la segmentation de plus en plus fine. Selon la CNIL, bien que ces apports rendent effectivement de nombreux services, cette personnalisation est aussi « *susceptible d'affecter des logiques collectives essentielles à la vie de nos sociétés* », des logiques telles que le pluralisme démocratique et culturel à titre d'exemples [101].

Ces techniques de profilage mises en place personnalisent la manière dont les individus accèdent aux informations et au contenu à tel point, que cette pratique s'apparente à du *microciblage*. Ce terme a été utilisé pour la première fois dans un contexte de lobbying politique

[96] KALTHEUNER (F.), BIETTI (E.), « Data is power: Towards additional guidance on profiling and automated decision-making in the GDPR », *Journal of Information Rights Policy and Practice* [en ligne], vol. 2 n° 2, janvier 2018, p. 4, [consulté le 3 août 2021].
[97] *Ibid*.
[98] ANGWIN (J.), MATTU (S.), PARRIS (T.), « Facebook Doesn't Tell Users Everything It Really Knows About Them », *Propublica* [en ligne], 27 décembre 2016, [consulté le 3 août 2021].
[99] MENDOZA-CAMINADE (A.), « Big data et données de santé : quelles régulations juridiques ? », *RLDI*, n° 127, 1er juin 2016.
[100] CONSTINE (J.), « Facebook Lets Advertisers Tap Purchase Data Partners To Target Customers, Categories Like Car-Buyers », *Techcrunch* [en ligne], 27 février 2013, [consulté le 3 août 2021].
[101] Rapport de la CNIL, *Comment permettre à l'Homme de garder la main ? Les enjeux éthiques des algorithmes et de l'intelligence artificielle*, *op.cit.*, p. 7.

lors des élections présidentielles aux États-Unis[102]. Le microciblage peut se décliner en deux variantes, le microciblage commercial, et le microciblage politique, qui n'ont donc pas le même objectif. La première variante est utilisée par l'écosystème de la publicité, tandis que la seconde variante sera utilisée par des annonceurs non commerciaux, à savoir les mouvements politiques et idéologiques, les partis politiques, candidats, ou organisations ayant un intérêt à diffuser du contenu tendant à influencer les idées politiques.

Ce microciblage est utilisé et mis en place par les systèmes de recommandation des différentes plateformes dans ces deux principaux buts, et avec l'appui des nouvelles techniques d'intelligence artificielle. Comme un avis du CEPD de 2018 le relevait, « *le microciblage peut passer par la façon dont les plateformes de médias sociaux choisissent quel contenu apparait sur le fil d'actualités d'une personne et dans quel ordre* »[103]. L'avis du CEPD précisait dans le cadre des conséquences de l'utilisation de ce type de pratique, que même si les conséquences du point de vue de l'individu peuvent être minimes sur certaines personnes, « *la complexité de la technologie à l'œuvre, les faibles niveaux de confiance et les intentions affichées de plusieurs grands acteurs de la technologie indiquent l'existence d'une culture de la manipulation dans l'environnement en ligne* »[104].

Ces microciblages préalables à la recommandation prennent une importance grandissante dans la mesure où les groupes politiques (mais aussi plus simplement le marché publicitaire), ont recours de plus en plus à l'analyse des données dans un objectif d'influence[105], mais aussi de propagation d'informations trompeuses selon un rapport de l'université d'Oxford[106].

La hiérarchisation et classification du contenu ne se résume pas à l'exercice d'une influence sur les individus. D'autres pratiques peuvent tout aussi bien impacter le marché de la concurrence. Ces dernières, impliquant la manipulation des recommandations, n'utilisent pas forcément le profilage et microciblage des individus. Dès lors, il apparait pertinent de les évoquer séparément.

---

[102] BODO (B.), HELBERGER (N.), VREESE (C. H.) « Political micro-targeting », *Internet Policy Review* [en ligne], vol. 6 n° 4, 20 décembre 2017, [consulté le 3 août 2021].
[103]CEPD, *Avis du CEPD sur la manipulation en ligne et les données à caractère personnel*, *op. cit.*, p. 11.
[104] *Ibid*.
[105] DOBBER (T.), TRILLING (D.), HELBERGER (N.) et al., « Two crates of beer and 40 pizzas: the adoption of innovative political behavioural targeting techniques », *Internet Policy Review* [en ligne], vol. 6 n° 4, 18 octobre 2017, [consulté le 3 août 2021].
[106] WOLLEY (S.), HOWARD (P.), *Computational Propaganda Worldwide: Executive Summary* [en ligne], rapport du Computational propaganda Research Project, 2017, p. 8, [consulté le 3 août 2021].

## II – Des pratiques anticoncurrentielles trouvant leur source dans la manipulation des recommandations

Il est communément admis que les marchés du numérique sont sujets à une extrême domination par certains acteurs. À titre d'exemple, Google représente plus de 90% du marché des moteurs de recherche, Facebook occupe encore 75% du marché des réseaux sociaux, et enfin, ces deux acteurs détiennent à eux seuls plus de la moitié du marché de la publicité en ligne dans son ensemble[107]. Par cette position particulière, ces acteurs sont devenus vitaux pour les professionnels. Il est dorénavant difficile pour un hôtel de ne pas avoir recours à la plateforme Booking et à son système de référencement. Ces opérateurs qualifiés de *keystones* (pierres angulaires) occupent une place centrale dans l'écosystème numérique. Google en tant que *keystone* fournit non seulement sa puissance et ses différentes infrastructures (moteurs de recherche, Google Analytics, EdgeRank, etc..) mais se positionne elle-même dans le marché convoité par ses utilisateurs professionnels en proposant ses propres outils, tel que des comparateurs de prix.

De surcroit, Google peut être qualifié de Gatekeeper (contrôleur d'accès au marché) puisqu'il remplit les conditions de cette qualification posées par la jurisprudence européenne, à savoir l'exercice d'un quasi-monopole sur les biens de l'infrastructure, le caractère indispensable de l'infrastructure pour l'accès à la clientèle, et l'impossibilité de répliquer cette infrastructure dans des conditions économiques raisonnables[108]. De manière générale, les GAFAM répondent à cette qualification, et sont par conséquent tributaires du devoir de garantir l'accès à leurs services dans des conditions équitables, non discriminantes et transparentes. Ce devoir fait référence à la théorie dite des « *facilités essentielles* », dont la portée a été étendue au fonctionnement des écosystèmes numériques depuis une décision *Microsoft* de 2004[109].

Par leur poids conséquent, les GAFAM exercent une position dominante dans de nombreux secteurs numériques : Google détient les moteurs de recherche, Microsoft les systèmes d'exploitation, Facebook les réseaux sociaux, et Amazon le E-commerce[110]. Cette notion de

[107] CLAUDEL (E.), « Numérique : le droit de la concurrence français à l'offensive », *RTD Com.*, 2020, p. 806.
[108] CJCE, 6 ch., 26 novembre 1998, *Oscar Bronner GmbH & Co. KG c. Mediaprint Zeitungs*, aff. C-7/97.
[109] Commission européenne, 24 mars 2004, *Microsoft*, aff. C-3/37.792.
[110] BOURREAU (M.), PERROT (A.), « Plateformes numériques : réguler avant qu'il ne soit trop tard », *Notes du conseil d'analyse économique* [en ligne], vol. 60 n° 6, 2020, pp. 1-12, [consulté le 4 août 2021].

position dominante a été définie en 1978 par la Cour de Justice des Communautés Européenne (CJCE) – l'ancienne Cour de Justice de l'Union Européenne (CJUE) – comme étant « *une position de puissance économique détenue par une entreprise qui lui donne le pouvoir de faire obstacle au maintien d'une concurrence effective sur le marché en cause en lui fournissant la possibilité de comportements indépendants dans une mesure appréciable vis-à-vis de ses concurrents, de ses clients et, finalement, des consommateurs.* »[111].

La position dominante n'est pas sanctionnable en tant que telle au sens du Droit de la concurrence. En revanche, une entreprise en position dominante est soumise à la responsabilité de ne pas porter atteinte à la concurrence par les mérites ainsi qu'à une concurrence effective et non faussée. À ce titre, l'abus de position dominante est sanctionné par le Traité sur le Fonctionnement de l'Union Européenne (TFUE), un traité fondamental destiné à organiser l'Union européenne et à déterminer son domaine de compétence au sein des États-Membres[112]. Ainsi, il est « *interdit, dans la mesure où le commerce entre États membres est susceptible d'en être affecté, le fait pour une ou plusieurs entreprises d'exploiter de façon abusive une position dominante sur le marché intérieur ou dans une partie substantielle de celui-ci.* »[113].

Les pratiques mises en causes peuvent ne causer aucun préjudice pour le consommateur, voire lui être favorables à court terme. Néanmoins, ces pratiques peuvent porter préjudice à la concurrence libre, qui sur le long terme, aboutira à une réduction du potentiel d'innovation des services. Les grandes plateformes ont un avantage de terrain puisqu'elles ont la possibilité technique de maitriser l'environnement numérique[114]. Certaines pratiques anti-concurrentielles passent par les systèmes de recommandation des services. Les modifications à l'échelle individuelle sont minimes, mais peuvent aboutir à de graves conséquences à l'échelle d'un marché.

À titre d'illustration, la manipulation du référencement du contenu proposé par les plateformes, et notamment les moteurs de recherche, est une pratique susceptible d'être caractérisée d'abus de position dominante. Il en est le cas notamment lorsque cette manipulation est utilisée à des

[111] CJCE, 14 février 1978, *United Brands et United Brands Continentaal c/ Commission*, aff. C-27/76.
[112] Traité sur le Fonctionnement de l'Union Européenne (TFUE), art. 1.
[113] TFUE, art. 102.
[114] DE MARCELLIS-WARIN (N.), MARTY (F.), THELISSON (E.) et al., « Intelligence artificielle et manipulations des comportements de marché : l'évaluation ex ante dans l'arsenal du régulateur », *Revue internationale de droit économique* [en ligne], vol. XXXIV n° 2, 2020, pp. 203-245, [consulté le 4 août 2021].

fins d'éviction des concurrents. Cette pratique, nommée *Self-preferencing* (ou auto-préférence), a été définie par l'Organisation de coopération et de développement économiques (OCDE) comme étant une stratégie par laquelle une entreprise dominante tire parti de sa position dominante sur un marché pour favoriser ses propres produits[115].

L'un des exemples les plus notables de l'utilisation de cette stratégie est l'affaire *Google Shopping* en date du 27 juin 2017[116]. Dans cette affaire, Google a été condamné à une amende de 2,4 milliards d'euros pour une favorisation illégale de son comparateur de prix Google Shopping. Il a notamment été reproché à Google d'abuser de sa position dominante en rétrogradant de façon artificielle le référencement des comparateurs de prix de ses concurrents[117]. Cet abus ne visait donc pas à acquérir une position dominante, mais plutôt à conserver la position dominante que Google détient depuis maintenant 2007 dans la plupart des marchés nationaux.

Il est intéressant de souligner que depuis 2010 déjà, l'Autorité française de la concurrence avait dénoncé les possibles pratiques de manipulation des scores concernant la publicité en ligne[118]. En effet selon cet avis de 2010, certains sites s'étaient plaints d'irrégularités concernant l'évolution de leur classement ou score de qualité[119]. En outre, le comparateur de prix de Google shopping apparaissait à la première page, tandis que les comparateurs des concurrents n'apparaissant que très loin, jusqu'à plusieurs pages après la première[120]. Puisqu'il est admis que seul 0,78% des clics se font sur la deuxième page de recherche[121], un tel contrôle du résultat de recherche revient à rendre totalement invisibles les concurrents. Finalement, cet abus était bien le résultat d'algorithmes de Google ayant dégradé les positions des concurrents afin de réduire leur visibilité pour le consommateur.

---

[115] MARTY (F.), « Pratiques anticoncurrentielles algorithmiques : une revue de littérature », *Groupe de recherche en Droit, Économie et Gestion (Gredeg)* [en ligne], Université Côte d'azur, 2021, p. 28, [consulté le 4 août 2021].
[116] Commission européenne, 27 juin 2017, *Moteur de recherche Google (Shopping)*, aff. AT.39740.
[117] PRIETO (C.), « Nouveaux abus de position dominante de Google : après celui lié à Google Shopping, ceux relatifs à Android », *RTD eur.*, 2018, p. 513.
[118] AUTORITE DE LA CONCURRENCE, *Avis n° 10-A-29 du 14 décembre 2010 sur le fonctionnement concurrentiel de la publicité en ligne* [en ligne], p. 59 [consulté le 3 août 2021].
[119] *Ibid.*, p. 59.
[120] BENSAMOUN (A.) (dir.), LOISEAU (G.) (dir.), *Droit de l'intelligence artificielle*, *op. cit.*, p. 183.
[121] ROPARS (F.), « SEO : les taux de clics et les performances des liens selon la position dans les SERPs », *Blog du modérateur* [en ligne], 28 août 2019, [consulté le 3 août 2021].

Les années suivantes, d'autres décisions concernant l'abus de position dominante de Google sont tombées, infligeant 4,34 milliards d'euros d'amendes lors de la décision *Google Android*[122] de 2018, et 1,49 milliard pour *Google AdSense*[123] en 2019. Au sein de cette dernière décision, l'enquête préalable de la Commission européenne a permis de conclure que Google avait la possibilité de « *contrôler le degré d'attractivité, et donc le taux de visite, des publicités contextuelles concurrentes* »[124]. Ce contrôle était en pratique exercé par un certain nombre de clauses, dont une obligeant les éditeurs à recueillir un accord de Google afin de modifier leurs publicités. Une telle pratique pouvait avoir un impact important pour les publicitaires dépendant totalement de Google pour la mise en avant de leur contenu publicitaire.

Le constat de ces différents abus, que ce soit en matière de recommandations mais aussi plus généralement des pratiques anticoncurrentielles basées sur les algorithmes eux-mêmes, ont conduit le législateur européen à envisager de nouvelles réformes. Il en est ainsi pour les propositions de législation sur les marchés numériques et sur les services numériques (DSA et DMA) soumis par la Commission européenne le 15 décembre 2020. Les différentes dispositions envisageant l'encadrement des grandes plateformes et les algorithmes de recommandation feront l'objet d'une analyse au sein du présent mémoire.

Il a été vu que de nombreuses pratiques pouvaient être mises en place afin de manipuler les recommandations pour les individus, qui pouvaient éventuellement atteindre le secteur de la concurrence. Il apparait pertinent maintenant de constater que certains droits sont menacés par ces différentes pratiques trouvant leur source dans l'usage des systèmes de recommandation.

[122] Commission européenne, 18 juillet 2018, *Google Android*, aff. AT.40099.
[123] Commission européenne, 20 mars 2019, *Google Search (AdSense)*, aff. AT.40411.
[124] COMMISSION EUROPEENNE, « Antitrust: la Commission inflige une amende de 1,49 milliards d'euros à Google pour pratiques abusives en matière de publicité en ligne », communiqué de presse [en ligne], Bruxelles, 20 mars 2019, [consulté le 3 août 2021].

## SECTION 2 – LA CARACTERISATION DES RISQUES POUR LES DROITS ET LIBERTES DES INDIVIDUS DU FAIT DE L'USAGE DES SYSTEMES DE RECOMMANDATION

Aujourd'hui, les plateformes optimisent la présentation du contenu en ligne afin de capter l'attention et d'augmenter leurs recettes. Aussi, la manipulation des systèmes de recommandation, couplée à un abus de l'utilisation des systèmes publicitaires peut alimenter une désinformation dangereuse pour la démocratie. Il apparait donc intéressant d'analyser les différentes conséquences liées à ces systèmes sous le prisme des droits fondamentaux, et des droits de la protection des données.

L'analyse des différents risques pour les droits sera principalement axée sur les individus pour deux raisons. D'une part, les atteintes caractérisées pour le marché et les professionnels s'en tiennent au droit de la concurrence et de façon encore trop généraliste sur les algorithmes, avec notamment l'étude des *collusions algorithmiques*[125] qui ne concerne que subsidiairement les algorithmes de recommandation en particulier. D'autre part, comme le professeur Jianqing Chen le soulignait récemment, si des études sur les aspects techniques (ainsi que sur les aspects démocratiques) des systèmes de recommandation ont été effectuées, les recherches sur les implications économiques de ces systèmes sont encore limitées[126].

Le choix a donc été fait de se concentrer sur les risques relatifs aux individus, et non aux usages pouvant porter préjudice aux professionnels. Afin d'apporter une vision globale de ces risques, il sera vu dans un premier temps les risques pour les droits fondamentaux du fait de l'usage des systèmes de recommandation (I). Enfin, de façon plus spécifique, les risques pour les droits de la protection des données personnelles seront traités (II).

# I – Les risques pour les droits fondamentaux du fait de l'usage des systèmes de recommandation

[125] V. par exemple pour les risques de collusion à l'aide d'algorithmes : AUTORITE DE LA CONCURRENCE, BUNDESKARTELLAMT, *Algorithmes et concurrence*, Novembre 2019. Disponible en ligne : [en ligne] [Consulté le 2 août 2021].

[126] UNIVERSITÉ DU TEXAS À DALLAS, « Recommended for you: Role, impact of tools behind automated product picks explored: Pros, cons of recommender systems. », *ScienceDaily*, 4 mars 2021. Disponible en ligne : https://www.sciencedaily.com/releases/2021/03/210304145157.htm [Consulté le 3 août 2021].

Les différentes pratiques en matière de ciblage des individus et de manipulation du contenu mettent en danger certains droits fondamentaux. L'un des premiers risques à envisager pour les droits fondamentaux concerne le pluralisme des médias. La liberté des médias et leur pluralisme est un droit protégé à l'article 11 de la Charte des droits fondamentaux[127]. Ces libertés sont intimement liées au droit à la liberté d'expression tel qu'il est garanti à l'article 10 de la Convention européenne des droits de l'Homme (CESDH)[128].

Un Comité d'experts du Conseil de l'Europe a fait le lien entre le droit à la liberté et au pluralisme des médias, et l'impact des systèmes de recommandation. Le Comité retient deux choses à ce sujet. Premièrement, l'exposition sélective aux contenus médiatiques induits par les phénomènes de bulles de filtres et de chambres d'écho peut « *entrainer une fragmentation et une polarisation accrue de la société* ». Deuxièmement, le « *contrôle grandissant sur le flux, la disponibilité, la facilité de recherche et l'accessibilité des informations et d'autres contenus en ligne* » des intermédiaires d'Internet est un fait préoccupant concernant le pluralisme des médias[129].

De plus, l'avis du CEPD sur la manipulation en ligne des données fournit deux arguments supplémentaires pour considérer ce risque. En effet, un contenu indexé par une plateforme sera *de facto* moins susceptible d'être vu par les individus. Or, les algorithmes de recommandation peuvent *« présenter un biais vis-à-vis de certains types de contenu ou de fournisseurs de contenu, risquant ainsi d'affecter les valeurs afférentes telles que le pluralisme et la diversité des médias* »[130]. Le deuxième argument tendant vers ce risque pour le pluralisme des médias tient au fait que les plateformes ont une réelle capacité à influencer les avis par la recommandation de contenu. Comme il a été vu précédemment, il en a été le cas lors des élections présidentielles américaines de 2016. Ainsi, « *La question est moins de savoir si les plateformes en ligne prétendument dominantes font (délibérément ou non) usage de leur pouvoir pour influencer les votes que le fait qu'elles ont, en principe, la capacité d'influer sur les processus de prise de décision politique* »[131].

[127] Charte des Droits Fondamentaux de l'Union européenne, art. 11, 2.
[128] Convention de sauvegarde des droits de l'Homme et des libertés fondamentales du 4 novembre 1950, art. 10.
[129] CONSEIL DE L'EUROPE, *Recommandation CM/Rec(2018)11 du Comité des Ministres aux États membres sur le pluralisme des médias et la transparence de leur propriété* [en ligne], 7 mars 2018, [Consulté le 3 aout 2021].
[130] CEPD, *Avis du CEPD sur la manipulation en ligne et les données à caractère personnel*, *op. cit.*, p. 16.
[131] *Ibid.*

Ce dernier argument renvoie tout aussi bien au pluralisme des médias, qu'au droit à des élections libres. Ce droit est garanti, entre autres, par l'article 3 du Protocole I de la CESDH. En outre, ce droit aux élections libres se caractérise notamment par le fait que les individus aient librement accès aux informations. En effet, « *une élection libre est une élection (…) où l'électorat a de réelles options et librement accès à des informations concernant ces options* » selon un rapport de la Commission de Venise en date de 2010[132]. Au sein de ce droit à l'élection libre, les grandes plateformes et réseaux sociaux ont une grande importance pour permettre aux électeurs de faire un choix « *réel et éclairé* »[133]. Cependant, cette montée des réseaux sociaux ainsi que le recours à des algorithmes tels que des systèmes de recommandation peuvent servir à menacer ce droit à des élections libres selon une étude de Benjamin Wagner de 2017[134].

De plus, ce droit ne peut pas être considéré comme respecté si les électeurs ont un risque d'être manipulés par les algorithmes, et ne bénéficient pas d'informations suffisantes sur l'élection en cours. Plus précisément, pour qu'une élection soit réellement démocratique, il est nécessaire de faire valoir sans discrimination, ni restrictions, « *la liberté de rechercher, de recevoir ou de communiquer des informations ou des idées afin que les électeurs puissent faire le choix éclairé nécessaire à la libre expression de leur volonté* »[135]. Ce droit, se rapportant à la liberté d'expression politique, peut être étendu au droit à l'information de manière générale et non seulement politique, du fait de l'impact des recommandations sur tout type de contenu, qu'il soit politique, culturel, ou commercial.

Ce droit d'informer, et surtout d'être informé dans le cadre des systèmes de recommandation[136], trouve notamment sa source en droit européen à l'article 10 de la CESDH, mais aussi à l'article 11 de la Déclaration des Droits de l'Homme et du Citoyen (DDHC)[137] en droit national, qui permet d'assurer la libre communication des pensées et des opinions. Si la notion de droit à l'information n'est pas explicitement consacrée en droit français, elle se dégage (au moins

---

[132] COMMISSION EUROPEENNE POUR LA DEMOCRATIE PAR LE DROIT (COMMISSION DE VENISE), *Rapport sur le calendrier et l'inventaire des critères politiques d'évaluation d'une élection* [en ligne], CDL-AD(2010)037, Strasbourg, 21 octobre 2010, p. 5, [consulté le 4 août 2021].
[133] *Ibid*.
[134] WAGNER (B.), *Étude sur les dimensions des droits humains dans les techniques de traitement automatisé des données (en particulier les algorithmes) et éventuelles implications réglementaires* [en ligne], Conseil de l'Europe, Comité d'experts sur les intermédiaires d'internet (MSI-NET), 6 octobre 2017, pp. 33-36, [Consulté le 7 aout 2021].
[135] COMMISSION EUROPEENNE POUR LA DEMOCRATIE PAR LE DROIT (COMMISSION DE VENISE), *Rapport sur le calendrier et l'inventaire des critères politiques d'évaluation d'une élection*, *op. cit.*, p. 5.
[136] POULLET (Y.), *Vie privée, liberté d'expression et démocratie dans la société numérique*, Larcier, 2020, p. 162.
[137] Déclaration des droits de l'homme et du citoyen du 27 août 1789, art. 11.

implicitement) par une construction prétorienne du Conseil constitutionnel[138]. En effet, le juge constitutionnel a fait du droit à l'information un principe du droit de la communication, en consacrant un droit des individus à recevoir une information diversifiée, et un accès à « *un nombre suffisant de publications de tendances et de caractères différents »*[139]. Il en est de même pour le pluralisme des courants d'expression socioculturels, érigé au rang d'objectif à valeur constitutionnelle[140].

Il va de soi que l'effet des bulles de filtre et des chambres d'écho amplifié par les systèmes de recommandation va, de par sa nature intrinsèque, à l'opposé du droit des individus à recevoir une information diversifiée. Ce lien est encore plus évident depuis qu'il est démontré que certains algorithmes de recommandation, notamment celui de Facebook, avaient avec le temps une tendance dégénérative en termes de variété de contenus proposés[141].

À la vue de ces différents droits, plusieurs interrogations légitimes se posent. Est-il acceptable de confier aux systèmes de recommandation des grandes plateformes le soin de décider de l'information qu'un individu sera susceptible de consulter ? En considérant les critères de priorisation axés sur une logique de rentabilité purement commerciale, qui « *accroît mécaniquement la diffusion de contenus clivant ou douteux* »[142] selon les dires du Sénat, rien n'est moins sûr.

Quand bien même la recommandation serait une nécessité technique face à l'immense flux d'information dont les individus sont destinataires, est-il justifié de ne pas leur laisser de réelles possibilités techniques et juridiques de contrôle du flux de ces informations ? Les actuelles options de configuration en matière de cookies ne sont pas suffisantes pour éviter les techniques de *profilage* et de *microciblage* portant atteinte à la vie privée des individus, et ne permettent que de réduire légèrement le caractère intrusif des publicités ciblées et contenus recommandés. D'autant plus que la pratique des *cookies walls*, consistant en une obligation d'accepter les cookies (ou de payer) pour accéder à un site, a été *in fine* validée par le Conseil d'État[143]. Cette

[138] DURIEUX (E.), *Droit des médias*, LGDJ, 8e ed., 2018, p. 60.
[139] Cons. const., 11 octobre 1984, n° 84-181 DC, cons. 34.
[140] Cons. const., 18 septembre 1986, n° 86-217 DC, cons. 11.
[141] JIANG (R.), CHIAPPA (S.), LATTIMORE (T.) et al., « Degenerate Feedback Loops in Recommender Systems », *Proceedings of AAAI/ACM Conference on AI, Ethics, and Society* [en ligne], janvier 2019, p. 1, [consulté le 4 août 2021].
[142] SENAT, *Avis politique sur la désinformation en ligne et les atteintes aux processus électoraux* [en ligne], Paris, 18 mars 2021, cons. 50, [consulté le 3 août 2021].
[143] CE, 19 juin 2020, *Association des agences-conseils en communication et autres*, n° 434684.

validation a par ailleurs été critiquée par le rapporteur public, estimant que rien n'empêchait le CE de considérer que le RGPD prohibait les *cookies walls* et ainsi valider les lignes directrices de la CNIL qui portaient cette interdiction[144], en tant que simple rappel de droit souple[145].

Enfin, il peut aussi être mentionné quelques spécificités techniques. Les options de navigation privées des navigateurs ne permettent pas le confort d'une navigation simple et se révèlent inefficaces dès lors qu'il est nécessaire d'utiliser un compte pour accéder à une plateforme telle que Facebook, Twitter, ou Instagram. Certains outils, tels que les *agrégateurs de Flux RSS*[146], ne sont encore utilisés que marginalement et s'avèrent être inutiles dans le cadre des grandes plateformes. En conclusion de cette interrogation, il n'existe donc que quelques solutions permettant de réduire l'impact des systèmes de recommandation et le traçage, mais encore aucune (dans la technique et le droit contemporain) qui permette à l'utilisateur de contrôler efficacement le flux de contenu auquel il sera sujet en navigant sur les différentes plateformes. Le risque d'atteinte est donc bien réel, si ce n'est omniprésent, face à ces systèmes préjudiciables au droit à la pluralité d'informations.

En plus de ces atteintes relatives à la vie sociale, culturelle et politique des individus, les conséquences gravitant autour de l'usage des systèmes de recommandation sont susceptibles de porter atteinte plus spécifiquement à l'autonomie personnelle et au consentement des individus.

## II – La mise en brèche du consentement et de l'information par le traitement des algorithmes de recommandation

Le traitement de données personnelles des individus dans une finalité de recommandation pose de légitimes questions en matière de consentement.

De manière générale, le consentement est, – comme certains auteurs le rappellent – une déclinaison de la liberté individuelle, qui se traduit par l'expression d'une volonté de

[144] V. en ce sens : CNIL, « Cookies et autres traceurs : la CNIL publie des lignes directrices modificatives et sa recommandation », 1 octobre 2020, [en ligne], [consulté le 3 août 2021].
[145] LALLET (A.), conclusions sur CE, 19 juin 2020, *Association des agences-conseils en communication et autres*, n° 434684.
[146] Il s'agit d'un logiciel, ou d'une application web, permettant d'agréger l'actualité sélectionnée selon les configurations de l'utilisateur, lui permettant d'effectuer une veille ciblée.

s'engager[147]. La liberté individuelle, qui conduit à nécessiter le consentement des individus pour toute action susceptible de leur porter atteinte (sauf si l'ordre public et l'intérêt général l'exige), trouve sa source dans de nombreux textes fondamentaux, dont la DDHC[148], ou encore la Charte des droits fondamentaux de l'Union européenne[149]. La référence au consentement, omniprésente au sein de nombreuses branches du droit, se trouve aussi plus spécifiquement dans le droit relatif aux données personnelles.

Sonia Desmoulin-Canselier et Daniel Le Métayer soulèvent un paradoxe intéressant en matière de consentement : Si la libre détermination des engagements est de plus en plus contestée dans différentes branches du droit, en limitant l'effet de certaines clauses et en accordant des protections aux parties faibles (en droit de la consommation notamment), le consentement au traitement des données personnelles tient un rôle déterminant[150]. Or, l'asymétrie informationnelle entre les utilisateurs et les plateformes faisant usage des données personnelles des individus aux fins de recommandation est bien réelle, et le déséquilibre entre les deux parties est tout aussi important.

Dans une utopie où le consentement serait acquis légitimement par les grandes plateformes, le consentement serait libre, spécifique, éclairé et univoque selon les termes du RGPD[151]. Chaque personne doit avoir la possibilité de retirer son consentement à tout moment, mettant fin aux traitements futurs mais conservant la licéité des traitements antérieurs[152]. Le consentement étant l'une des six bases légales nécessaires au traitement licite, son non-respect rendrait le traitement illégitime et violerait par conséquent l'article 6 du RGPD. En pratique, les plateformes telles que Facebook et Instagram fondent la personnalisation du contenu et des publicités sur le consentement des utilisateurs, comme en atteste leur politique de confidentialité[153].

---

[147] DESMOULIN-CANSELIER (S.), LE METAYER (D.), *Décider avec les algorithmes : Quelle place pour l'Homme, quelle place pour le droit ?*, *op. cit.* note 77, p. 117.
[148] DDHC, art. 1, 2, et 4.
[149] Charte des droits fondamentaux de l'Union européenne, art. 6.
[150] DESMOULIN-CANSELIER (S.), LE METAYER (D.), *Décider avec les algorithmes : Quelle place pour l'Homme, quelle place pour le droit ?*, *op. cit.* note 77, pp. 118-119.
[151] RGPD art. 4. 11.
[152] *Ibid.*, art. 7.
[153] V. en ce sens l'onglet spécifique aux bases légales utilisées par Facebook, et par extension Instagram, au sein de leur politique de confidentialité, révisée pour la dernière fois le 21 août 2020, [en ligne], [consulté le 5 août 2021].

Pour autant, – et surtout en matière d'algorithmes – les qualités inhérentes au consentement sont rarement remplies en pratique, et les traitements aux fins de recommandation et de contenu ciblé n'y font pas exception pour plusieurs raisons.

En premier lieu, le caractère « libre » du consentement pour ces finalités est discutable, car l'utilisation de services tels que Twitter, Facebook (et par extension Instagram) peuvent parfois être une nécessité pour la vie sociale, mais aussi pour d'autres raisons personnelles ou professionnelles. De plus, en l'absence de réelles alternatives à ces services, il est parfois compliqué de pouvoir s'en passer. Pourtant, le RGPD précise bien que le consentement ne doit pas être considéré comme donné librement si la personne concernée « *n'est pas en mesure de refuser ou de retirer son consentement sans subir de préjudice* »[154]. Le consentement est-il donc réellement libre pour des réseaux sociaux tels que Facebook ou Twitter, considérés aujourd'hui en fait comme en droit, comme des espaces publics parfois indispensables[155] ?

En second lieu, le caractère « éclairé » du consentement pourrait tout aussi bien faire débat, du fait qu'avec la complexité des systèmes d'intelligence artificielle, la diversité des sources de collecte, et l'opacité de ces systèmes parfois appelés « boites noires »[156], ces derniers rendent le consentement « éclairé » plus difficile à obtenir. En effet concernant les systèmes de recommandation, les prédictions produites souffrent souvent de cet effet de « boite noire », ce qui rend difficile l'analyse des raisons qui ont poussé le système à recommander un contenu pour le concepteur même du modèle[157]. Si l'aspect technique n'est pas connu, le caractère éclairé du consentement pour ce type de finalité apparait tout aussi illusoire par rapport à l'information sur l'impact de ces systèmes dès lors que, selon les termes de la CNIL, « *l'absence de compréhension claire par les individus du fonctionnement des plateformes qu'ils utilisent pour s'informer, notamment, fait partie intégrante du problème* »[158]. Ainsi, une étude a montré

[154] RGPD, cons. 42.
[155] FORTEZA (P.), « Reprendre le contrôle des réseaux sociaux », *Fondation Jean Jaurès* [en ligne] , 8 décembre 2020, [consulté le 5 août 2021].
[156] Terme utilisé pour désigner l'opacité du processus de traitement de données opéré par certains algorithmes d'intelligence artificielle. V. en ce sens : GEORGES (B.), « Le talon d'Achille de l'intelligence artificielle », *Les échos* [en ligne], 15 mai 2017, [consulté le 5 août 2021].
[157] V. notamment : GROSSETTI (Q.), « Système de recommandation sur les plateformes de micro-blogging et bulles filtrantes », *Réseaux sociaux et d'information* [en ligne], thèse, Sorbonne Université, 2018, p. 39, [consulté le 5 août 2021].
[158] CNIL, *Comment permettre à l'homme de garder la main ? Les enjeux éthiques des algorithmes et de l'intelligence artificielle. op.cit.*, p. 36.

que plus de 60% des utilisateurs de Facebook n'avaient « *aucune idée de l'activité éditoriale que joue effectivement l'algorithme* »[159].

Ces problématiques liées au consentement ont donné lieu à certains conflits concernant le contenu publicitaire ciblé. Il y a quelques années déjà, le *Financial Times* révélait que Google avait violé sa politique de confidentialité ainsi que les principes de consentement et de transparence pour envoyer du contenu ciblé. Dans les faits, Google mettait en place un traqueur permettant d'identifier les internautes, tout en invitant les annonceurs à accéder à une page Web permettant de connaitre l'activité des utilisateurs, ce qui leur permettait de leur envoyer des publicités ciblées[160]. Plus récemment, l'autorité de protection des données Luxembourgeoise a prononcé une amende de 746 millions à la société Amazon[161]. Compte tenu de la législation luxembourgeoise interdisant la publicité d'une décision avant l'épuisement des voies de recours, cette dernière est encore privée. Il est en revanche admis à l'heure actuelle qu'Amazon a été sanctionné pour avoir notamment imposé un ciblage publicitaire des individus sans leur consentement libre[162].

En 2018 aussi, une plainte collective signée par 10 000 personnes et issue de la Quadrature du Net a été adressée à la CNIL contre Google et le service YouTube. Il était reproché à ces services Google d'obtenir le consentement de façon non libre puisque le traitement établi pour proposer des recommandations et du contenu personnalisé se basait sur une analyse comportementale qui n'était pas nécessaire à une utilisation normale des services, et pourtant liée à leur utilisation[163]. Le 25 mai 2021, la Quadrature du Net est revenue sur cette plainte, considérant que la condamnation par la CNIL en date du 21 janvier 2019[164] ne répondait même pas aux demandes de la plainte en ne s'adressant pas au bon service, tout en ne réglant pas la question du consentement forcé[165]. La Quadrature du Net n'a pas manqué de critiquer le trop

[159] *Ibid.*
[160] POULLET (Y.), FRENAY (B.), *Rapport et propositions de recommandations sur le « Profilage et la Convention 108+ du Conseil de l'Europe* [en ligne], Conseil de l'Europe, T-PD(2019)07, Strasbourg, 9 septembre 2019, p. 32, [consulté le 5 août 2021].
[161] CNIL, « L'autorité luxembourgeoise de protection des données a prononcé à l'encontre d'Amazon Europe Core une amende de 746 millions d'euros », 3 août 2021, [en ligne], [consulté le 5 août 2021].
[162] LA QUADRATURE DU NET, « Amende de 746 millions d'euros contre Amazon suite à nos plaintes collectives » [en ligne], 30 juillet 2021, [consulté le 5 août 2021].
[163] TREGUER (F.), « réclamation contre Google », *La Quadrature du Net* [en ligne], 28 mai 2018, [consulté le 5 août 2021].
[164] CNIL, 21 janvier 2019, délibération n°SAN-2019-001.
[165] LA QUADRATURE DU NET, « Les GAFAM échappent au RGPD, la CNIL complice », [en ligne], 25 mai 2021, [consulté le 5 août 2021].

faible montant de l'amende, et l'inaction de la CNIL à ce sujet. Il serait compliqué de contredire cette critique. La CNIL, qui ne serait plus que « *l'ombre d'elle-même* »[166] selon leurs dires, a sanctionné Google à hauteur de 50 millions d'euros, soit 3 heures de leur chiffre d'affaires de l'époque. Une bien mince compensation comparée à la mise en brèche du consentement de milliards d'individus utilisant leurs services, et lorsque le RGPD leur permet notamment d'infliger une sanction à hauteur de 4% de leur chiffre d'affaires mondial pour une violation des principes du consentement lié au traitement[167]. Cependant, cette tendance est à nuancer, compte tenu du montant élevé de l'amende prononcée par la Commission Nationale pour la Protection des Données luxembourgeoise à l'égard d'Amazon, l'espoir de nouvelles sanctions véritablement dissuasives reste de mise.

Le microciblage politique évoqué précédemment détient lui-aussi ses problématiques relatives à la protection des données. Ce dernier implique la collecte et la combinaison de données personnelles d'individus à grande échelle dans l'objectif de déduire certaines sensibilités politiques et préférences. Selon certains auteurs, de telles pratiques « *peuvent violer les règles de protection des données personnelles et, en outre, être utilisées à des fins inattendues et parfois nuisibles* »[168]. Une évidence apparait, l'usage des techniques de microciblage, exploitation permettant aux algorithmes de recommandation de gagner en efficacité, effectuent un traitement de données politiques.

Bien que l'exploitation des données préalables à la recommandation ne renvoie pas nécessairement à des données politiques, elles peuvent le devenir par leur croisement ou regroupement avec d'autres informations et pistages effectués sur Internet et sur les plateformes. Comme deux membres de la CNIL l'évoquaient en 2019, la personnalisation du contenu qui suit la collecte de ces informations, peut être source de problèmes lorsqu'elle oriente l'opinion politique des personnes concernées par le traitement[169].

---

[166] LA QUADRATURE DU NET, « Amende de 746 millions d'euros contre Amazon suite à nos plaintes collectives », *op. cit.* note 162.
[167] RGPD, art. 83. 5.
[168] SHULGA-MORSKAYA (T.), SANTOS (N.), « Les invisibilités » dans les campagnes électorales en ligne : quel encadrement juridique ? », p. 182, dans : NEVEJANS (N.), *Données et technologies numériques*, ed. Mare & Martin, coll. Droit et Science politique, 2021, 350 p.
[169] SERUGA-CAU (E.), HAVEL (T.), « Campagne électorale et utilisation des données personnelles : grands principes et points de vigilance », *AJCT* [en ligne], février 2019, p. 75, [consulté le 4 août 2021].

Ces données politiques sont considérées comme des données sensibles. Protégées au titre du RGPD, relèvent de « *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* »[170]. Le traitement de ces données est en principe interdit, à quelques exceptions près. L'une de ces exceptions, applicable au type de traitement envisagé par ces systèmes algorithmiques, est le recueil du consentement explicite de la personne concernée par le traitement[171], un consentement supplémentaire qui s'additionne sans se substituer à la base légale.

Concernant la publicité personnalisée, le consentement explicite précédant la collecte a pourtant été malencontreusement oublié par Google concernant certaines données sensibles, bien qu'il ait été affirmé par la politique de confidentialité que Google n'affichait pas « *d'annonces personnalisées en fonction de catégories sensibles* »[172]. Il semble pourtant naturel de considérer que les catégories publicitaires validées par Google, telles que « *cancer* », ou encore *« male impotence* »[173] (du français : dysfonctions érectiles), soient de près ou de loin, des données sensibles concernant la santé ou la vie sexuelle des individus. Plusieurs plaintes ont été déposées auprès des autorités de protection des données à propos de Google et du système d'enchères en temps réel, ou *Real-time bidding* (RTB)[174] pour violation des règles de protection des données. Plusieurs preuves ont été soumises sur le site du célèbre moteur de recherche *Brave***,** attestant de l'utilisation de données très sensibles sans recueil d'un quelconque consentement explicite, tout en soulignant les défaillances en matière de sécurité du RTB[175]. Cependant, aucune action

[170] RGPD, art. 9.1.
[171] *Ibid*., art. 9.2.a.
[172] V. en ce sens : Politique de confidentialité de Google, « Proposer des services personnalisés, notamment en matière de contenu et d'annonces », [en ligne] , mis à jour au 1er juillet 2021, [consulté le 6 août 2021]. Il est à noter que cette mention était déjà présente dans la politique de confidentialité du 22 janvier 2019, précédant donc les plaintes adressées contre Google et le système RTB, [en ligne], [consulté le 6 août 2021].
[173] KALLENBORN (G.), « Malade du SIDA, drogué, victime de viol… comment les publicitaires nous catégorisent », *01Net* [en ligne], 28 janvier 2019, [consulté le 6 août 2021]. V. pour plus de précisions : RYAN (J.), « Update on GDPR complaint (RTB ad auctions) », *Brave* [en ligne], 28 janvier 2019, [consulté le 6 août 2021].
[174] Ce système était à l'origine de plus de 51% de la publicité ciblée en 2018. V. en ce sens : POILVE (B.), « Les enchères en temps réel (RTB), un système complexe », *Laboratoire d'innovation numérique de la CNIL* [en ligne], 14 janvier 2020, [consulté le 6 août 2021].
[175] V. en ce sens un lien répertoriant les preuves publiées, et adressées aux autorités de protection des données irlandaises et anglaises : https://brave.com/rtb-evidence/ [consulté le 6 août 2021].

n'a été entreprise à ce sujet du fait de l'inaction des autorités de protection, et l'affaire n'a pas évolué depuis 2020[176].

Ces garanties n'ont pas non plus l'air d'être mises en place concernant la recommandation de contenu politique (entre autres) sur la plateforme YouTube, qui respecte elle-aussi les règles de confidentialité de Google. Il pourra être constaté que le visionnage de contenu sur YouTube par exemple, sera influencé par les recommandations, qui elles-mêmes sont issues de prédictions basées sur des centres d'intérêts qui peuvent être politiques. Ensuite, cette agrégation de données et la prédiction vers des centres d'intérêts politisés, se font bel et bien (Il y a donc un traitement de données sensibles au sens du RGPD), et en l'absence de consentement explicite[177]. Ce résultat vient du fait que le contenu politisé, affiché aux utilisateurs par les algorithmes de recommandation, se fait sans aucune distinction du type de contenu, qu'il soit commercial, politique, ou culturel.

Tous ces risques, qu'ils soient liés aux droits fondamentaux ou à la protection des données, nécessitent donc des garanties de taille. Avant de voir quels seront les prochains apports législatifs en la matière, il apparait intéressant de voir quels outils sont déjà mis en place afin de protéger les individus face aux conséquences de la personnalisation du contenu.

[176] RYAN (J.), « The ICO's failure to act on RTB, the largest data breach ever recorded in the UK », *Brave* [en ligne], 17 janvier 2020, [consulté le 6 août 2021].

[177] V. par exemple en navigation privée, l'absence de recueil du consentement explicite sur la page d'accueil de YouTube. La seule indication relative au traitement de données à des fins de recommandation de contenus est la suivante : « *ils* [publicités et contenus personnalisés] *peuvent être basés* (…) *sur votre activité, par exemple vos recherches Google et les vidéos YouTube que vous regardez. Il s'agit par exemple de résultats et de recommandations plus pertinents, d'une page d'accueil YouTube personnalisée et d'annonces publicitaires adaptées à vos centres d'intérêt.* »

# CHAPITRE 2 – UN DROIT CONTEMPORAIN INADAPTE AUX SYSTEMES DE RECOMMANDATION

Les effets des systèmes de recommandation, disposant d'un potentiel de manipulation aussi redoutable pour les individus que pour la collectivité[178], ont été résumés de la manière suivante par le philosophe Gaspard Koenig : « *L'abêtissement du débat public, l'hystérie partisane, la dictature de l'émotion, le retour de la morale publique et la désinformation de masse sont des conséquences directes du titillement permanent que les réseaux sociaux exercent sur nos circuits neuronaux.* »[179]. Ainsi, les recommandations – et la source principale de revenus des grandes plateformes, la publicité ciblée – se joueraient du cerveau humain en instaurant des *nudges*[180], de subtiles modifications de l'environnement permettant de faire suggérer un comportement à l'humain, pensant qu'il décide un acte par lui-même.

C'est un constat plutôt pessimiste après la mise en perspective des différentes pratiques et effets issus du fonctionnement de recommandations portées sur la maximisation du profit, et de leurs conséquences. Un troisième acteur entre dès lors en jeu, à savoir le régulateur. La réponse juridique est-elle satisfaisante compte-tenu des circonstances énoncées ? Des progrès sont encore à faire, et se font attendre pour les réglementations à venir. Pour autant, certains outils juridiques ont été mis en place au cours de ces dernières années permettant de combattre certains effets néfastes des systèmes de recommandation, ainsi que pour apporter une transparence et loyauté accrue des plateformes envers leurs utilisateurs. Certaines réponses sont issues du droit de la protection des données. Il sera vu néanmoins que ces dispositions se révèlent parfois inadaptées à la problématique du contenu recommandé (Section 1). Enfin, les obligations de contrôle et de transparence incombant aux plateformes marquent certes, une avancée pour le respect des individus, mais restent encore insuffisantes (Section 2).

---

[178] POULLET (Y.), RUFFO DE CALABRE (M.-N.), « La régulation des réseaux sociaux », *op. cit* note 90.

[179] KOENIG (G.), *La fin de l'individu : voyage d'un philosophe au pays de l'intelligence artificielle*, ed. L'observatoire, 2019, p. 151.

[180] V. en ce sens pour une plus large définition : THALER (R.), SUNSTEIN (C.), *Nudge: Improving Decisions About Health, Wealth, and Happiness*, Yale University Press, 2008, p. 6, « *Le nudge* […] *est un aspect de l'architecture du choix qui modifie le comportement des gens d'une manière prévisible sans leur interdire aucune option ou modifier de manière significative leurs motivations économiques. Pour ressembler à un simple « coup de pouce », l'intervention doit être simple et facile à esquiver. Les « coups de pouce » ne sont pas des règles à appliquer. Mettre l'évidence directement sous les yeux est considéré comme un coup de pouce. Interdire uniquement ce qu'il ne faut pas faire ou choisir ne fonctionne pas.* ».

## SECTION 1 – DES REPONSES INADAPTEES EN MATIERE DE PROTECTION DES DONNEES

À n'en pas douter, le RGPD est une véritable fierté européenne concernant la protection des données personnelles. Son champ d'application très étendu et la mise en place de nombreux principes gouvernant le traitement des données personnelles en fait l'incarnation des principes européens en matière de droits fondamentaux. Plusieurs pays à travers le monde s'inspirent du RGPD afin d'établir leur propre règlementation[181], et il n'existe à ce titre aucune volonté des régulateurs européens de revenir en arrière[182]. Cependant, certains principes établis par le RGPD se révèlent antinomiques au fonctionnement des algorithmes. Il sera donc vu dans un premier temps quels sont les points généraux d'inadaptation de la protection des données face aux systèmes algorithmiques (I). Dans un second temps, il sera vu que certains droits prévus explicitement en matière de profilage, peinent à s'appliquer en pratique lorsqu'il s'agit de profilage aux fins de recommandation de contenu (II).

### I – Les points généraux d'inadaptation de la protection des données face aux systèmes algorithmiques

Une première inadaptation peut relever tout simplement du champ d'application du RGPD. Ce dernier s'appliquant uniquement aux traitements de DACP, certaines utilisations de l'IA pourraient passer outre cette règlementation. En effet, le RGPD n'est applicable que lorsque des DACP sont en jeu. Ces données, définies par le RGPD comme toute information se rapportant à une personne physique identifiée ou identifiable[183], sont aussi des données qui permettent « *d'individualiser* » les individus au sens du Conseil d'État[184], reprenant certains critères énoncés par l'ancien G29, devenu le Comité européen de protection des données[185].

[181] V. notamment : GRECO DE MARCO LEITE (G.), BOUGRINE (A.), « La nouvelle loi brésilienne sur la protection des données personnelles inspirée du RGPD européen », *UggcAvocats* [en ligne], 18 juin 2019, [consulté le 9 août 2021].
[182] GEROT (M.), MAXWELL (W.), « Le RGPD pourrait freiner les ambitions de l'Europe en matière d'intelligence artificielle », *Gaz. Pal.*, 23 juin 2020, n° 381k0, p. 16.
[183] RGPD, art. 4. 1.
[184] CE, 8 février 2017, *JCDecaux France*, n° 393714, cons. 7.
[185] GROUPE DE TRAVAIL « ARTICLE 29 » SUR LA PROTECTION DES DONNEES, *Avis 05/2014 sur les Techniques d'anonymisation* [en ligne], 10 avril 2014, [consulté le 9 août 2021].

Si les informations traitées ne relèvent pas de ce concept de DACP, il est possible de s'affranchir du respect de ces principes pour les systèmes d'IA qui ne dresseraient que des prédictions de comportement pour des groupes généraux d'individus, ainsi que pour des DACP qui auraient été anonymisées[186].

Par exemple, les cookies, bases de données, et autres informations d'activité (comme les vidéos YouTube regardées, ou l'activité sur des applications ou sites tiers) stockées par Google pour attribuer des recommandations sont effectivement protégées[187]. Cependant, le RGPD, par sa limitation au traitement de DACP, ne permet pas d'encadrer les méthodes de recommandation du contenu, alors qu'elles pourraient avoir un impact tout aussi important que les autres fonctionnalités.

À ce titre, même si pour Google, l'exploitation de son moteur de recherche est qualifiée de traitement de DACP[188], le RGPD n'apportera pas de réponse adaptée sur le fait que les résultats du moteur Google recommandent plus facilement des informations relatives à des actes criminels pour les recherches d'information sur des noms plus courants au sein de minorités ethniques[189]. Ces problèmes, qui peuvent venir d'un comportement indésirable de l'algorithme, ou être qualifiés de *biais algorithmiques,* touchent tout autant les systèmes de recommandation que d'autres utilisations des algorithmes.

Comme second point d'inadaptation, certains des principes du RGPD tels que le principe de minimisation de la collecte des données[190], s'avèrent opposés au développement des algorithmes, et à une recommandation de contenu efficace. Préalablement à la recommandation, la phase d'apprentissage de ces algorithmes de *machine learning* – et encore davantage pour le *deep learning* – nécessitent la collecte massive de données afin d'établir certains modèles prédictifs. La garantie de ces principes est donc loin d'être adaptée à cet usage des données des

[186] *Ibid*., p. 13. Une donnée est considérée comme anonymisée, s'il n'est pas raisonnablement possible de procéder à une individualisation, corrélation, ou inférence de ces données vers un individu en particulier.
[187] V. en ce sens : Politique de confidentialité de Google, « Informations que nous collectons via nos services », [en ligne], mis à jour au 1er juillet 2021, [consulté le 6 août 2021].
[188] CE, 19 juillet 2017, *Google Inc.*, n° 399922.
[189] BEN-ISRAEL (I.), CERDIO (J.), EMA (A.) et al., *Vers une régulation des systèmes d'IA* [en ligne], CAHAI – Comité ad hoc sur l'intelligence artificielle, 2020, p. 148, [consulté le 9 août 2021].
[190] RGPD, art. 5. 1. c).

utilisateurs, ce qui aboutit tout simplement à un respect relatif de ce principe du fait que seul un certain degré de minimisation puisse être respecté[191].

Face à cette problématique de la minimisation, une difficulté supplémentaire propre aux algorithmes de recommandation survient. En effet, certaines solutions permettant de mieux respecter le principe de minimisation ont été proposées lorsque le traitement est réalisé par une IA, mais ne s'appliquent pas forcément à ces algorithmes particuliers.

Par exemple, le responsable de traitement pourrait utiliser un jeu de données synthétiques[192] pour entrainer l'algorithme, ou encore de réduire les données redondantes ou marginales non nécessaires pour les performances de l'algorithme[193]. Si la seconde technique pourrait être mise en place, l'emploi de jeux de données synthétiques s'avère particulièrement compliqué pour les algorithmes de recommandation. Du fait de leur objectif particulier et de leur fonctionnement hautement personnalisé, la performance de ces algorithmes dépend énormément des données fournies par chaque utilisateur unique, et se base sur l'activité de ces derniers. En somme, il existe autant de modèles de recommandation qui s'améliorent en temps réel que d'utilisateurs, et le fonctionnement de l'algorithme reste similaire entre les individus, mais doit sans cesse s'adapter en fonction des données de l'utilisateur visé[194].

Cette mesure étant donc peu envisageable pour garantir ce principe, le choix semble davantage s'imposer entre une performance de l'algorithme qui absorberait énormément de données en contrepartie, ou une résignation de l'utilisateur à en faire un usage limité.

À l'instar du respect relatif du principe de minimisation, le principe de finalités souffre aussi de lacunes lorsque le traitement est réalisé par l'IA, puisqu'il n'est pas toujours bien déterminé. Selon le RGPD, les finalités d'un traitement de DACP se doivent d'être déterminées, explicites

---

[191] CONSEIL DE L'EUROPE, *Intelligence artificielle et protection des données : enjeux et solutions possibles* [en ligne], T-PD(2018)09Rev, Strasbourg, 25 janvier 2019, p. 8, [consulté le 7 août 2021].

[192] *Ibid.*, p. 9, « Les données synthétiques sont générées à partir d'un modèle de données construit sur la base de données réelles. Elles devraient être représentatives des données réelles initiales »

[193] COMITE CONSULTATIF DE LA CONVENTION POUR LA PROTECTION DES PERSONNES A L'EGARD DU TRAITEMENT AUTOMATISE DES DONNEES A CARACTERE PERSONNEL, *Lignes directrices sur la protection des personnes à l'égard du traitement des données à caractère personnel à l'ère des mégadonnées* [*en ligne*], T-PD(2017)01, Strasbourg, 23 janvier 2017, section 4, pt. 4.3, [consulté le 9 août 2021].

[194] Les méthodes de *clustering* (amas) de certains algorithmes de recommandation permettent de regrouper les différents contenus en groupes de goûts. Mais pour placer l'utilisateur au sein de ces groupes afin de lui recommander le contenu qu'il préfère, ses propres données doivent être collectées. V. en ce sens : D'ASCOLI (S.), *Comprendre la révolution de l'intelligence artificielle*, *op. cit.*, p. 79.

et légitimes[195]. Cependant, l'IA pose certains problèmes pour la détermination de ces finalités, surtout lorsqu'elle sert à la sélection de contenu pour les utilisateurs. Un rapport de 2020 précisait à ce titre que les « *moteurs de recherche, systèmes de recommandation de vidéos et agrégateurs d'informations sont souvent opaques non seulement sur les données qu'ils utilisent pour sélectionner ou hiérarchiser les contenus, mais aussi sur les finalités d'une telle sélection* »[196].

Pour de nombreux algorithmes, il est parfois compliqué de déterminer avec succès la finalité du traitement du fait que les résultats, prédictions ou inférences obtenus par l'algorithme d'IA pourraient être totalement imprévus et découverts en cours de processus[197]. Il existe aussi un risque lorsque l'utilisation des données permettant l'entrainement de l'algorithme se trouve décontextualisée de son objectif de base. Un exemple de décontextualisation notable serait l'algorithme *Predpol*, qui a été inspiré d'un algorithme conçu initialement pour prédire les séismes, mais dont le modèle a été finalement utilisé pour prédire les lieux au risque d'infraction élevé[198].

Le problème dans le cadre des systèmes de recommandation, serait plus particulièrement axé sur un risque de détournement de finalités au détriment des individus. Initialement, les finalités principales de ces systèmes sont de fournir un contenu pertinent pour les utilisateurs à l'aide du profilage, mais aussi de personnaliser les annonces publicitaires afin de faire fonctionner le modèle économique de ces plateformes. Néanmoins, il existe le risque (plutôt évident) qu'au-delà de ces finalités, ce traitement soit aussi présent afin de permettre aux algorithmes de recommandation de maintenir les utilisateurs le plus longtemps possible, peu importe l'objectivité, la qualité ou l'intérêt de ce contenu. Cette manœuvre, si elle était qualifiée, pourrait être considérée comme un détournement de finalité, qui est sanctionné par le RGPD, mais aussi pénalement[199].

Cet intérêt pour le maintien de l'attention menace donc le strict respect des finalités du ciblage comportemental aux fins de recommandation. Il soulève l'ambiguïté que les plateformes

[195] RGPD, art. 5. b).
[196] BEN-ISRAEL (I.), CERDIO (J.), EMA (A.) et al., *Vers une régulation des systèmes d'IA*, *op. cit.* note 189, p. 27.
[197] GAULLIER (F.), « Le principe de finalité dans le RGPD : beaucoup d'ancien et un peu de nouveau », *CCE*, n°4 dossier 10, avril 2018.
[198] COUVELAIRE (L.), « Le logiciel qui prédit les délits », *Le monde* [en ligne], 4 janvier 2013, [consulté le 9 août 2021].
[199] CP, art. 226-21.

peuvent laisser quant à la réelle exploitation de ces données, et appelle ainsi à un plus grand contrôle de leur utilisation[200], qui est susceptible d'atteindre l'élaboration des opinions au profit du sensationnalisme. Par ailleurs, il aurait pu être attendu du RGPD que de véritables droits concernant le profilage aux fins de recommandation soit établis. Pourtant, ces dispositions se révèlent tout aussi inadaptées.

## II – L'inadaptation plus spécifique de l'encadrement du profilage face aux systèmes de recommandation

Comme il a été vu précédemment, les systèmes de recommandation utilisés par les grandes plateformes ont recours aux techniques de profilage, notamment pour prédire les préférences personnelles, les intérêts des utilisateurs et leur comportement. Il convient dans un premier temps de souligner le fait que le RGPD a permis la mise en place de nombreuses protections et mesures de transparence en matière de profilage.

À titre d'illustration, le droit à l'information prévu par le RGPD est censé s'appliquer aux personnes faisant l'objet d'un profilage par ces algorithmes[201]. Rappelant l'expression de Judith Rochfeld qui parlait de « *droits minimaux de la personne algorithmée* »[202], les personnes concernées doivent en théorie donner leur consentement clair et explicite, et disposent en cas de profilage, du droit de s'opposer à cette pratique[203]. En outre, le principe de protection de la vie privée dès la conception (*privacy by design*), et par défaut (*privacy by default*) devrait s'appliquer lors de la mise en place de ces techniques à des fins de recommandation. De ce droit à l'information découle l'obligation pour le responsable du traitement de fournir les informations nécessaires (identité du responsable de traitement, finalités du traitement, base légale, etc..) lorsqu'il s'agit d'un profilage[204]. Plus encore lorsque le profilage se base sur des données sensibles, le RGPD prévoit que « *La prise de décision et le profilage automatisés fondés sur des catégories particulières de données à caractère personnel ne devraient être autorisés que dans des conditions spécifiques.* »[205].

---

[200] DELTORN (J.-M.), « La protection des données personnelles face aux algorithmes prédictifs », *RLDF 2017* [en ligne], chron. n°12, [consulté le 9 août 2021].
[201] RGPD art. 13.
[202] ROCHFELD (J.), « L'encadrement des décisions prises par algorithme », *Dalloz IP/IT, 2018,* pp. 474
[203] SCARAMOZZINO (E.), « Le profilage encadré pour favoriser la diversité culturelle », *Dalloz JAC 2016*, n° 36, p. 6.
[204] RGPD, art. 13.2.f).
[205] RGPD, cons. 71.

D’autres renforcements ont été mis en place pour un profilage moins intrusif de manière générale. À titre d’exemple, la collecte d’information et les traceurs utilisés pour le profilage, notamment les cookies, ont fait l’objet de lignes directrices en France par la CNIL[206], et la jurisprudence de la Cour de justice de l’Union européenne a aussi joué un rôle à ce sujet. Cette dernière a notamment eu à rappeler certaines évidences telles que l’illicéité des cases pré-cochées pour le placement de cookies à des fins de tracking publicitaire[207]. Les protections et mesures de transparence sont donc loin d’être absentes, mais force est de constater que certaines dispositions auraient eu le mérite d’être mieux adaptées aux systèmes de recommandation ayant recours au profilage. La principale déception provient de l’article 22 du RGPD.

Cet article 22 accorde un droit concernant les décisions fondées exclusivement sur un traitement automatisé faisant usage du profilage. En effet, la personne concernée par un traitement « *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.* »[208]. Ces systèmes relèvent par exemple des outils de justice prédictive, ou encore d’algorithmes utilisés par l’administration tels que l’algorithme *Parcoursup*. Les domaines de la justice, de la police, de l’administration et de la médicine sont assurément couverts par ce droit lorsque les individus sont susceptibles de subir des effets juridiques.

Sans considérer d’effets juridiques à proprement parler, un algorithme portant une atteinte significative aux individus pourrait aussi suffire à faire valoir ce droit. C’est le cas par exemple pour le respect de la vie privée, droit fondamental protégé tant en droit national[209] qu’européen[210]. Cette atteinte à la vie privée peut même résulter de l’exploitation par des algorithmes de données en libre accès selon l’interprétation de Desmoulin-Canselier et Le Métayer[211] d’une jurisprudence de la Cour de cassation[212]. C’est un élément intéressant, lorsqu’il a été admis par une étude portant sur les utilisateurs de Twitter que « *La personnalité*

[206] CNIL, *recommandation proposant des modalités pratiques de mise en conformité en cas de recours aux « cookies et autres traceurs »*, délibération n° 2020-092, 17 septembre 2020, [consulté le 9 août 2021].
[207] CJUE, 1 octobre 2019, *Verbraucherzentrale Bundesverband eV c/ Planet49 GmbH*, Aff. C-673/17.
[208] RGPD, art 22.1.
[209] C. civ., art. 9.
[210] CEDH, art. 8.
[211] DESMOULIN-CANSELIER (S.), LE METAYER (D.), *Décider avec les algorithmes : Quelle place pour l’Homme, quelle place pour le droit ?*, *op. cit.* note 77.
[212] Cass. 1e. civ., 18 octobre 2017, n° 16-19.740.

*d'un utilisateur peut être facilement et fidèlement déduite de ses données publiques* »[213]. En effet, si même une atteinte à la vie privée peut résulter de l'exploitation de données en libre accès, il peut tout aussi bien en être le cas pour l'exploitation très intrusive des algorithmes de recommandation qui exploitent parfois des données très sensibles.

Malheureusement, même en présence d'une atteinte de ce type, ainsi que pour les atteintes mentionnées précédemment, ce droit est inadapté à l'usage du profilage à des fins de recommandation. En effet, ce droit est certes applicable au profilage, mais uniquement pour les systèmes de prise de décisions automatisées. Or, si la notion de profilage est très large, le RGPD ne couvre que les décisions fondées exclusivement sur un traitement. De ce fait, un processus automatisé aboutissant à une recommandation, et non une décision, ne se verra pas contraint de fournir ce droit aux personnes concernées par le traitement[214].

A l'instar de l'article 22 du RGPD qui met en place un droit de ne pas faire l'objet de décisions entièrement automatisée, il aurait pu être imaginé dès la mise en place du RGPD l'existence d'un droit de ne pas faire l'objet de recommandations substantiellement basées sur le profilage. Là où l'évaluation du préjudice pour la décision automatisée est plutôt axée sur le préjudice individuel de la personne concernée par le traitement, l'importance des effets des algorithmes de recommandation est d'autant plus visible lorsque les risques collectifs sont envisagés.

C'est l'idée qu'évoquait la CNIL en 2017, lorsqu'elle énonçait dans son rapport sur l'IA à propos des phénomènes de bulles de filtre et de chambres d'écho, le préjudice possible à l'échelle de la société en ces termes : « *les formes de privation d'exposition des individus à l'altérité, à des opinions différentes, des leurs, notamment dans le registre politique, pourraient en tout cas constituer, selon certains, un problème pour la qualité et la vitalité du débat public, pour la qualité et diversité de l'information, terreaux du fonctionnement correct des démocraties.* »[215].

En l'absence actuelle de ce droit, restent encore les garanties de transparence, et d'information, ainsi que le recueil du consentement pour les utilisateurs. Il est à noter que si l'encadrement du

[213] QUERCIA (D.), KOSINSKI (M.), STILLWELL (D.), « Our Twitter Prifles, Our Selves : Predicting Personality with Twitter », *Privacy, Security, Risk and Trust (PASSAT)* [en ligne], octobre 2011, p. 6, [consulté le 10 août 2021].
[214] BENSAMOUN (A.) (dir.), LOISEAU (G.) (dir.), *Droit de l'intelligence artificielle*, *op. cit.*, p. 283.
[215] CNIL, *Comment permettre à l'Homme de garder la main ? : Les enjeux éthiques des algorithmes et de l'intelligence artificielle*, *op. cit.* note 35, p. 35.

profilage aux fins de recommandation est inadapté, les législations à venir – qui seront traitées ultérieurement – semblent apporter une réponse plus satisfaisante et orientée spécifiquement vers les systèmes de recommandation et les options de profilage liées à ces derniers.

Enfin, il peut être aussi être souligné qu'une prise en compte du risque élevé de ces systèmes commence à faire surface, comme en témoigne une nouvelle piste pour une actualisation des recommandations sur le profilage[216], dont la dernière date de 2010[217]. Cette piste suggère au point n° 1 que le profilage puisse être considéré comme étant à risque élevé lorsqu'il « *entraine un risque de manipulation des personnes concernées* », ou a pour objet des données relevant de catégories particulières, et enfin, celui fait par des « *services d'information en ligne disposant d'une large part du marché, sur base de l'utilisation de leurs services* ». Le risque de manipulation, qui est aussi envisagé par le rapport conjoint de 2019[218] sur l'évolution de la situation du profilage depuis 2010, permettrait d'englober plus facilement les algorithmes de recommandation dans cette définition du risque élevé.

Il serait donc envisagé selon cette piste que ce type de profilage à risque élevé puisse faire l'objet d'une évaluation des risques individuels, mais aussi et enfin collectifs. Cette évaluation se ferait par une équipe multidisciplinaire, et par les représentants des intérêts concernés par le profilage, et donc, des représentants des personnes profilées eux-aussi, qui seraient déterminés par une certaine exigence de compétence pour le sujet[219].

En conclusion, si le droit contemporain de la protection des données présente certaines inadaptations face aux systèmes de recommandation, ces différentes prises de consciences nourrissent de vifs espoirs vers une adéquation des règles de protection des données. Au-delà de l'inadaptation de certaines de ces règles de protection des données pour les algorithmes, force est de constater que des insuffisances en matière de contrôle et de transparence du contenu recommandé sont présentes.

---

[216] POULLET (Y.), FRENAY (B.), *Profilage et la Convention 108+ : Pistes pour une actualisation* [en ligne], T-PD(2019)07bisrev, Conseil de l'Europe, Strasbourg, 7 novembre 2019, [consulté le 10 août 2021].

[217] Recommandation CM/Rec(2010)13, adoptée par le Comité des Ministres du Conseil de l'Europe le 23 novembre 2010, sur proposition du Comité européen de coopération juridique (CDCJ), [en ligne], [consulté le 10 août 2021].

[218] POULLET (Y.), FRENAY (B.), *Profilage et la Convention 108+ : Rapport sur l'évolution de la situation après l'adoption de la Recommandation(2010)13 sur le profilage* [en ligne], T-PD(2019)07rev, Conseil de l'Europe, Strasbourg, 7 novembre 2019, p. 31, [consulté le 10 août 2021].

[219] POULLET (Y.), FRENAY (B.), *Profilage et la Convention 108+ : Pistes pour une actualisation*, *op. cit.* note 216, pt. 8.6.

## SECTION 2 – LES INSUFFISANCES DE TRANSPARENCE ET DE CONTROLE EN MATIERE DE CONTENU RECOMMANDE

Sommes-nous entrés dans l'ère de la *« post-vérité »* ? Une question rhétorique à bien des égards, comme de nombreux auteurs le pensent. Néologisme démocratisé en 2004 par Ralph Keyes dans son livre intitulé *The Post-truth Era*[220], la *« post-vérité »* fait référence à « *des circonstances dans lesquelles les faits objectifs ont moins d'influence pour modeler l'opinion publique que les appels à l'émotion et aux opinions personnelles* »[221]. Cette formule provenant du Dictionnaire d'Oxford, a été consacrée comme mot de l'année en 2016 par ce dernier[222].

Les résultats de suggestion fournis par les systèmes de recommandation ne contrediront pas cette tendance. Il n'aura échappé à personne que l'actualité de la pandémie du Covid19 a été particulièrement sujette à la diffusion de fausses informations. Bien que de nombreux autres facteurs sont en jeu, il sera vu qu'une partie de la responsabilité de cette diffusion peut aussi être accordée à la logique de fonctionnement des systèmes de recommandations des plateformes. En 2016 déjà, ce reproche pouvait être fait lors des évènements de la campagne présidentielle de Donald Trump. La CNIL notamment, avançait que « *Les fake news, largement évoquées lors de la campagne menée par Donald Trump, si elles ne sont pas un produit direct des algorithmes, se diffusent et s'amplifient à l'intérieur des chambres d'écho constituées par les algorithmes des réseaux sociaux ou des moteurs de recherche.* »[223].

Même si leur propagation est amplifiée par les algorithmes de recommandation, les *Fakes News* existent depuis toujours. Il n'était pas nécessaire d'attendre l'arrivée d'une technologie aussi puissante pour que la plupart des enfants pensent par effet « boule de neige » que souffler dans leurs cartouches de Nintendo 64 aiderait à résoudre tout problème[224]. Le problème est à présent beaucoup plus dangereux, comme en témoigne l'opinion publique européenne, qui considère à

[220] Keyes (R.), *The Post-truth Era: Dishonesty And Deception In Contemporary Life*, ed. First, 2004, 312 p.
[221] Dictionnaire d'Oxford, définition de 2016 [en ligne], la définition actuelle a été simplfiée : « *relating to circumstances in which people respond more to feelings and beliefs than to facts* », [consulté le 6 août 2021].
[222] GATELAIS (S.), « "Post-vérité", élu mot de 2016 : de Trump au Brexit, le reflet d'une année populiste », *Le Nouvel Obs* [en ligne], 21 novembre 2016, [consulté le 6 août 2021].
[223] CNIL, *Comment permettre à l'Homme de garder la main ? : Les enjeux éthiques des algorithmes et de l'intelligence artificielle*, *op. cit.* note 35, p. 36.
[224] DE (F.), « On vous a menti ! Souffler dans les cartouches ne sert à rien ! », *Hitek* [en ligne], 3 juillet 2014, [consulté le 6 août 2021].

83% que les fausses informations sont un problème général pour la démocratie[225]. Il n'est pourtant pas exclu que les régulateurs, plateformes, voire même les utilisateurs, aient la possibilité de jouer un rôle important dans le contrôle des contenus considérés comme nuisibles, incluant notamment la désinformation en ligne, et les abus en matière de publicité ciblée.

Les fakes news ne sont pas le seul élément permettant de constater des insuffisances dans le contrôle du contenu recommandé. Il apparait tout aussi intéressant de voir que la délimitation en matière de publicité commerciale ou politique apparait de plus en plus complexe, et que des mesures de transparence à cet égard devraient être renforcées. En effet, ce contenu est lui aussi à même de modifier l'opinion des individus de manière subtile, d'autant plus lorsque certaines publicités politiques ciblées se maquillent en information standard, ou publicité traditionnelle.

Ces deux points d'intérêt ayant un rapport direct avec le façonnement des bulles de filtre des utilisateurs, les réponses juridiques en matière de lutte contre la manipulation de l'information seront traitées dans un premier temps (I). Il sera cependant vu dans un second temps en quoi ces réponses juridiques s'avèrent insuffisantes en matière de contrôle et de transparence, notamment du fait que ces règlementations gagneraient en efficacité en visant plus explicitement les algorithmes de recommandation (II).

## I – Les réponses juridiques en matière de lutte contre la manipulation de l'information

Au niveau national, de nouveaux mécanismes ont été introduits depuis les lois du 22 décembre 2018 relatives à la lutte contre la manipulation de l'information[226]. Deux dispositions ont été incluses au sein du Code électoral, l'une instaurant diverses obligations de transparence[227], tandis que l'autre instaure une nouvelle procédure de référé d'urgence dans les périodes de campagne électorale[228]. Ces deux articles sont opérationnels pendant les trois mois précédant un scrutin.

[225] COMMISSION EUROPEENNE, « Final results of the Eurobarometer on fake news and online disinformation », *Shaping Europe's digital future* [en ligne], 12 mars 2018, [consulté le 11 août 2021].
[226] Loi n° 2018-1201 du 22 décembre 2018 relative à la lutte contre la manipulation de l'information, et Loi n° 2018-1202 du 22 décembre 2018 relative à la lutte contre la manipulation de l'information.
[227] C. élect., art. L. 163-1.
[228] C. élect., art. L. 163-2.

Concernant les nouvelles obligations de transparence, l'article L. 163-1 du Code électoral prévoit lors de cette période que les opérateurs d'une plateforme en ligne[229] dont l'activité dépasse un seuil de 5 millions[230] de connexions sur le territoire français, et pour des contenus se rattachant à la campagne électorale, seront tenus de fournir une information loyale, claire et transparente sur l'identité de la personne physique ou de la personne morale qui verse à la plateforme des rémunérations en contrepartie de la promotion de contenus d'information.

Il peut être rappelé que des mesures de transparence dans le référencement des contenus publicitaires (lorsqu'un objectif de manipulation politique est présent) ont été exigées par la jurisprudence bien avant l'entrée en application de cette loi. Le Conseil d'État depuis 2009, considère que lorsque le référencement commercial d'un site électoral sur un moteur de recherche a pour finalité d'attirer des internautes sur le site, ce référencement sera considéré comme une publicité commerciale à des fins de propagande électorale[231], ce qui est interdit par le Code électoral[232]. Cette interprétation du référencement commercial à finalité électorale a été réitérée par le Conseil constitutionnel en 2017[233]. S'agissant de la source des revenus, le montant des rémunérations perçues doit être rendu public, et l'utilisateur doit être informé de l'usage de ses données.

Ensuite, une nouvelle procédure de référé d'urgence a été établie par les lois du 22 décembre 2018 relatives à la lutte contre la manipulation de l'information. L'article L. 163-2 du Code électoral permet en effet de saisir le tribunal judiciaire de Paris en référé, afin d'ordonner de mettre fin à toute diffusion par le biais d'un service de communication au public en ligne[234], des « *allégations ou imputations inexactes ou trompeuses d'un fait de nature à altérer la sincérité du scrutin* »[235]. Pour que cette action soit valable, il est nécessaire que les fausses

[229] C. consomm., art. L. 111-7, I, un opérateur de plateforme en ligne se définit comme « *toute personne physique ou morale proposant, à titre professionnel, de manière rémunérée ou non, un service de communication au public en ligne* » qui reposent notamment sur *« 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* ».
[230] Recommandation n° 2019-03 du 15 mai 2019 du Conseil supérieur de l'audiovisuel aux opérateurs de plateforme en ligne dans le cadre du devoir de coopération en matière de lutte contre la diffusion de fausses informations, [en ligne], [consulté le 11 août 2021].
[231] CE, 13 février 2009, *Élections municipales de la commune de Fuveau*, n° 317637.
[232] C. élect., art. L. 52-1.
[233] Cons. const., 8 décembre 2017, n° 2017-5026 AN, cons. 14.
[234] Loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique, art. 1, « *On entend par communication au public en ligne toute transmission, sur demande individuelle, de données numériques n'ayant pas un caractère de correspondance privée, par un procédé de communication électronique permettant un échange réciproque d'informations entre l'émetteur et le récepteur.* »
[235] C. élect., art. L. 163-2.

informations soient diffusées « *de manière délibérée, artificielle ou automatisée et massive* »[236].

Le Conseil constitutionnel a cependant émis une limitation à propos de cette procédure de référé. Afin d'éviter les abus, la fausse information se doit de remplir deux conditions cumulatives. Le référé ne pourra s'appliquer qu'aux informations dont le « *caractère inexact ou trompeur est manifeste* »[237], et la diffusion de cette information devra présenter un « *risque d'altération de la sincérité du scrutin* »[238] lui aussi manifeste.

La jurisprudence a ajouté à ce propos qu'une information, même si cette dernière fait l'objet d'une exagération, ne sera pas considérée comme manifestement inexacte ou trompeuse dès lors qu'elle n'est pas dénuée de tout lien avec des faits réels[239]. L'affaire concernait en l'espèce un message du Ministre de l'intérieur sur Twitter, évoquant avec exagération des attaques et blessures sur le personnel soignant d'un hôpital par des manifestants, alors qu'il s'agissait d'une intrusion.

Enfin, les plateformes en ligne soumises à ces dispositions se sont aussi vues attribuer un véritable « devoir de coopération » afin de lutter contre les fausses informations en ligne de manière générale, sans que cette lutte ne soit limitée aux périodes électorales[240]. Ce devoir implique que les plateformes mettent en place un dispositif de signalement des fausses informations. À cela s'ajoute des mesures portant sur la transparence des algorithmes utilisés pour ordonner, référencer et recommander les contenus. Par ailleurs, ces plateformes doivent publier des statistiques sur les fonctions de leurs différents algorithmes[241].

La CSA a aussi un rôle à jouer dans la lutte contre la désinformation dorénavant. En effet, la loi du 22 décembre 2018 permet aux CSA d'adresser des recommandations aux plateformes en ligne afin de mieux lutter contre la diffusion de fausses informations[242]. À ce titre, ce dernier s'est vu attribuer une mission générale de « *lutte contre la diffusion de fausses informations*

[236] *Ibid.*
[237] Cons. const., 20 décembre 2018, n° 2018-773 DC, cons. 23.
[238] *Ibid.*
[239] TGI Paris, 17 mai 2019, *Marie-Pierre Vieu et Pierre Ouzoulias c/ Twitter et Christophe Castaner*, n° RG 19/53935.
[240] Loi n° 2018-1202 du 22 décembre 2018, *op. cit.* note 226, art. 11.
[241] *Ibid*., art. 14.
[242] Loi n° 2018-1202 du 22 décembre 2018, *op. cit.*, note 226 art. 12.

*susceptibles de troubler l'ordre public ou de porter atteinte à la sincérité* » des scrutins[243]. Ce pouvoir reste pour l'instant un pouvoir de supervision sur le domaine des plateformes en ligne.

Du point de vue européen, certaines réponses orientées vers une logique d'autorégulation ont été formulées. La notion de désinformation du point de vue européen est plus large que la notion française. Elle inclut les informations dont on peut vérifier la fausseté et le caractère trompeur dans le but d'altérer la sincérité du scrutin, mais aussi dans un but lucratif ou dans une intention de tromper le public qui est susceptible de causer un préjudice public[244]. Tout comme la définition française, il est nécessaire d'établir la mauvaise foi ou l'intention délibérée de nuire afin d'éviter de potentielles censures en matière de critique, satire, parodie, droits de citation et autres.

Cette action se dirige essentiellement vers des campagnes de désinformation provenant de l'extérieure de l'UE, et se traduit par plusieurs mesures, comme la création d'un réseau de coopération européen, ou des orientations sur la protection des données personnelles dans le contexte politique. Concernant la transparence des plateformes, l'UE s'est positionnée dans une volonté d'autorégulation en mettant en place un code de bonnes pratiques signé par les principales plateformes en 2018[245].

Ce code comprend certaines mesures notables en matière de recommandations, telles que diluer la visibilité de la désinformation en améliorant la répétabilité de contenus fiables, ou encore des outils de signalement de fausses informations dans le cadre de la lutte contre les *fake news*, ainsi que des outils de transparence permettant de mieux comprendre les algorithmes utilisés dans l'organisation du contenu[246].

Cependant, malgré les progrès réalisés par ces réponses nationales et européennes, de nombreuses insuffisances relatives au contrôle et à la transparence restent à relever.

---

[243] Loi n° 86-1067 du 30 septembre 1986 relative à la liberté de communication (Loi Léotard), art. 17-2.
[244] COMMISSION EUROPEENNE, *Lutter contre la désinformation en ligne: une approche européenne* [en ligne], Communication de la Commission au Parlement européen, au Conseil, au Comité économique et social européen et au Comité des régions, COM/2018/236 final, [consulté le 11 août 2021].
[245] COMMISSION EUROPEENNE, *EU code of Practice on Disinformation* [en ligne], septembre 2018, [consulté le 12 août 2021].
[246] *Ibid*.

## II - Les insuffisances de contrôle et de transparence en matière de recommandation du contenu

Tout d'abord, le référé créé en droit national risque d'être compliqué à appliquer en pratique du fait de ses conditions très restrictives[247]. Ce référé ne permet pas non plus de lutter sur le plan macroscopique contre la désinformation.

Quant aux obligations de transparence prévues par le devoir de coopération, le CSA a publié une recommandation dans laquelle il invitait les plateformes visées à développer des outils de signalement accessibles et visibles, ainsi qu'à développer la transparence de leurs algorithmes de recommandation[248]. Plus précisément, le CSA encourageait à assurer la traçabilité des données des utilisateurs à des fins de recommandation et de hiérarchisation des contenus, mais aussi à développer une information claire, suffisamment précise et facilement accessible des critères (et de leur importance) conduisant à l'ordonnancement du contenu proposé. Cette information devait aussi être mise en place s'agissant des réglages permettant de personnaliser la recommandation des contenus, ainsi que pour les principaux changements des algorithmes de recommandation. Enfin, un outil de communication accessible permettant d'obtenir des informations personnalisées et précises sur le fonctionnement des algorithmes avait été demandé au sein de la recommandation.

Ce document n'ayant pas de valeur juridique contraignante, un bilan plutôt mitigé a été dressé en juillet 2020 concernant l'application effective des mesures demandées[249]. Si la plupart des plateformes ont mis en place un outil de signalement de fausses informations, les informations transmises quant aux moyens déployés se sont révélés insuffisantes et ne permettaient pas d'apprécier le respect des objectifs fixés par la loi. Ce n'était pourtant pas la disposition la plus compliquée à respecter. S'agissant de la transparence des algorithmes de recommandation, sans surprise, le CSA a exprimé ses regrets sur le manque d'informations transmises. Certaines déclarations fournissaient même un niveau de détail totalement identique à ce qui est mis à la disposition du public sur leurs sites[250]. En somme, des politiques de confidentialité évasives.

[247] RAMBAUD (R.), « lutter contre la manipulation de l'information », *AJDA 2019*, p. 453.
[248] CSA, 15 mai 2019, recommandation n° 2019-03, *op. cit.* note 230.
[249] CSA, *Lutte contre la diffusion de fausses informations sur les plateformes en ligne : bilan de l'application et de l'effectivité des mesures mises en œuvre par les opérateurs en 2019* [en ligne], juillet 2020, [consulté le 11 août 2021].
[250] Ibid., p.37.

Cela ne permet donc pas d'évaluer quels efforts ont été mis en place pour la « *construction d'un esprit éclairé chez les utilisateurs* ».

Certaines plateformes, notamment Facebook, se sont complètement jouées des recommandations en transmettant des informations sur les algorithmes permettant de déceler et de modérer les fausses informations, plutôt que de transmettre celles demandées sur leurs algorithmes de recommandation[251]. En bref et sans surprise, l'autorégulation basée sur des recommandations non contraignantes ne fonctionne pas dans ce cas de figure.

Naturellement, les mêmes insuffisances ont été constatées sur le plan européen. En 2019, le Groupe des régulateurs européens pour les services de médias audiovisuels a souligné lui aussi que des insuffisances subsistaient dans cette approche d'autorégulation. Cette insuffisance résultait du fait que le contrôle effectif de l'exécution des obligations des plateformes s'avérait encore lacunaire[252]. Le même constat que celui du CSA a pu être fait vis-à-vis du respect des dispositions du code de bonne conduite élaboré par la Commission européenne.

Certains auteurs soulignent une seconde problématique à cette approche européenne. Cette dernière se concentre effectivement sur les problématiques liées aux campagnes électorales, mais ne traite pas suffisamment les points d'ombre liés à la collecte et à l'exploitation des données des individus[253]. En effet, ces points d'ombre qualifiés « *d'invisibilités* » ont certes été davantage mis en lumière par les nouvelles dispositions sur le contrôle du contenu en ligne et des publicités, mais ne traitent pas plus la question des pratiques de *microciblage*, et de croisement entre les bases de données des acteurs du numériques.

Concernant le contenu publicitaire politique, bien que certaines mesures de transparence aient été mises en œuvre par les plateformes, il est encore à ce jour compliqué de déterminer l'origine des publicités politiques, ainsi que la source de leurs financements[254].

---

[251] *Ibid.*
[252] CSA, « Le CSA expose sa vision d'une nouvelle régulation européenne », *11e réunion de l'ERGA* [en ligne] , 27 juin 2019, [consulté le 7 août 2021].
[253] SHULGA-MORSKAYA (T.), SANTOS (N.), « Les invisibilités » dans les campagnes électorales en ligne : quel encadrement juridique ? », p. 187, dans : NEVEJANS (N.), *Données et technologies numériques*, *op. cit.* note 168.
[254] DOMMETT (K.), POWER (S.), « The Political Economy of Facebook Advertising: Election Spending, Regulation and Targeting Online », *The Political Quarterly* [en ligne], vol. 90 n° 2, avril 2019, p. 6, [consulté le 4 août 2021].

Du point de vue national comme européen, il apparait donc au vu des réactions que ces nouvelles dispositions ne prennent pas suffisamment en compte le rôle des algorithmes de recommandation, ce qui aboutit à l'exploitation par les plateformes de cette zone grise juridique. Cette prise en compte était pourtant implicitement encouragée dans de nombreuses études déjà. L'analyse de l'algorithme de recommandation de Facebook, ainsi que l'étude précédemment citée sur YouTube en introduction[255], montrait bien le rôle des algorithmes dans le cheminement des utilisateurs vers du contenu de plus en plus problématique afin de maintenir l'utilisateur sur la plateforme, ainsi que l'importance de l'algorithme contribuant à hauteur de 70% du contenu visionné sur la plateforme.

Une étude récente publiée en juillet 2021 (il ne pourra pas être reproché au législateur de ne pas avoir pris en compte des dernières statistiques) par Mozilla mentionnait que bien que le principal problème réside dans l'algorithme de recommandation. Il a été établi, en plus de confirmer les chiffres des précédentes études sur la plateforme YouTube, que les vidéos recommandées étaient 40% plus susceptibles d'être du contenu nuisible, ce qui inclut la désinformation ou des discours haineux et violents, et les escroqueries[256]. Toujours en 2021, un rapport du *Center for Countering Digital Hate* (CCDH) en lien avec l'omniprésence de la désinformation lors de la pandémie Covid-19, envisageait de mettre à jour les processus de la plateforme Instagram, conduisant aux théories du complot et à la désinformation à partir des systèmes de recommandation[257]. La logique de l'algorithme de Facebook est donc tout aussi similaire, leur algorithme de recommandation *News Feed* faisant la part belle aux contenus générant de nombreuses interactions[258] (ce qui est une caractéristique intrinsèque de l'actualité clivante et des fausses informations).

Il faut cependant nuancer le rôle des algorithmes dans le contexte particulier des *fake news*. S'ils participent bien à une recommandation plus élevée de contenus problématiques, clivants, et jouant sur l'affect, les algorithmes fonctionnent différemment selon les plateformes, et pour le cas des *fake news* et sur certaines plateformes, le comportement humain reste un facteur de propagation important. Sur la plateforme Twitter par exemple, le CSA a conclu en 2020 que les

[255] HORTA RIBEIRO (M.), OTTONI (R.), WEST (R.), et al., « Auditing Radicalization Pathways on YouTube », *op. cit.* note 52.
[256] MOZILLA, *YouTube Regrets : A crowdsourced investigation into YouTube's recommendation algorithm* [en ligne], juillet 2021, [consulté le 11 août 2021].
[257] CENTER FOR COUNTERING DIGITAL HATE, *Malgorithm : how instagram's algorithm publishes misinformation and hate to millions during a pandemic* [en ligne], 9 mars 2021, [consulté le 7 août 2021].
[258] ZUBOFF (S.), *L'âge du capitalisme de surveillance*, *op. cit.* note 9, p. 678.

abonnés de comptes « non fiables » avaient une tendance 10 fois à 20 fois plus élevée à partager le contenu considéré comme non fiable[259].

Cette grande différence de partage entre le contenu fiable et les fausses informations pourrait servir aux plateformes à repérer plus facilement ce contenu à l'aide d'algorithmes de détection automatique. D'autant plus que ces plateformes pourraient d'ores et déjà réellement disposer des outils pour se débarrasser des *fake news* selon des sources en lien direct avec les organes décisionnels de Facebook[260]. Néanmoins, il apparait utopique de penser que ce type de plateformes combattra avec autant d'hardiesse un élément constitutif de leur réussite économique sous la faible menace de mesures centrées sur une logique d'autorégulation.

De surcroit, tant que de véritables audits externes et contrôles des algorithmes utilisés n'auront pas été pris en compte dans la mesure de ces phénomènes, l'asymétrie informationnelle entre les individus et régulateurs, et les grandes plateformes restera en faveur des plateformes. Certains progrès ont été effectués, mais le bénéfice du doute à l'égard de leur bonne foi apparait compliqué, voire impossible lorsque leur radicale indifférence à l'égard des conséquences induites par leur logique de hiérarchisation du contenu transparait[261].

[259] CSA, *La propagation des fausses informations sur les réseaux sociaux : Étude du service Twitter* [en ligne], novembre 2020, p. 68, [consulté le 12 août 2021].
[260] NUNEZ (M.), « Facebook's Fight Against Fake News Was Undercut by Fear of Conservative Backlash », *Gizmodo*, 14 novembre 2016, [consulté le 11 août 2021].
[261] V. en ce sens : ZUBOFF (S.), *L'âge du capitalisme de surveillance*, *op. cit.* note 9, pp. 669-679. Une liste non exhaustive de différents exemples démontrant l'indifférence des grandes plateformes à l'égards des *fake new*s, du fait de leur intérêt économique directement associé à leur propagation, garantissant ainsi la valorisation toujours plus conséquente de données comportementales.

# CONCLUSION DE LA PREMIERE PARTIE

« *Est-il loyal de collecter, d'analyser et de commercialiser les données les plus intimes de l'individu « transparent », afin d'influencer ses opinions politiques, sur le fondement de son consentement non vraiment éclairé ou même explicite ?* »[262]

Les plateformes ont eu tout le loisir de s'adonner à des pratiques permettant de satisfaire une logique propre à l'économie de l'attention, et cela, en dépit des conséquences que pouvaient avoir la classification de contenus clivants, nuisibles, ou faussés sur les individus et la société dans son ensemble. Si le contenu isolé peut ne revêtir aucune illégalité manifeste en lui-même, il s'agit bien là de pointer du doigt le risque collectif qu'engendre une altération du débat public, et de la perception même que les individus pourraient avoir sur le monde du fait de règles algorithmiques. Cet effet ne touche pas uniquement les personnes physiques, mais peut par ailleurs porter atteinte au marché du fait de pratiques anticoncurrentielles exploitant les règles algorithmiques de classement et de référencement.

L'enfermement algorithmique, dérivé en concepts de *bulle de filtre* ou de *chambre d'écho*, n'a pas fait l'objet de règles protectrices spécifiques. Bien que le droit contemporain prévoit d'ores et déjà des règles de transparence, de contrôle, et un encadrement de la protection des données, les enjeux propres aux systèmes de recommandation se révèlent être dans un interstice, un carrefour entre ces éléments juridiques dispersés.

La portée infructueuse de ces dispositions envers les systèmes de recommandation revient en réalité à viser la conséquence d'un préjudice, plutôt que la cause, à savoir la configuration de l'algorithme pour une finalité néfaste. L'expansion de la diffusion des *fake news* constitue une bonne illustration des lacunes persistantes de transparence et de contrôle de ces algorithmes. En tout état de cause, il est nécessaire d'envisager de nouvelles mesures propres à ces systèmes. C'est précisément ce qu'un récent projet de règlement européen ambitionne d'accomplir.

[262] SHULGA-MORSKAYA (T.), SANTOS (N.), « Les invisibilités » dans les campagnes électorales en ligne : quel encadrement juridique ? », p. 187, dans : NEVEJANS (N.), *Données et technologies numériques, op. cit*. note 168.

# PARTIE 2 – VERS UN ENCADREMENT RENFORCE DES SYSTEMES DE RECOMMANDATION

Cela ne fait que depuis quelques temps que les régulateurs entreprennent la démarche d'identifier directement les mécanismes favorisant la manipulation délibérée de l'information. Là où les précédentes règlementations tentaient de corriger davantage la conséquence (le contenu publié) plutôt que la cause (les mécanismes algorithmiques favorisant la prolifération et visibilité du contenu nuisible), les réglementations à venir illustrent la prise de conscience : le fait que si ce contenu a été diffusé à une échelle aussi importante, cela a été fait avec l'aide non négligeable des algorithmes d'IA[263].

Au-delà de la compréhension des enjeux techniques, la politique européenne en matière de régulation de ces plateformes a marqué un réel tournant dernièrement. D'une logique d'autoréglementation consacrée par l'Union européenne au sein du *Code de bonnes pratiques contre la désinformation*[264], les derniers projets de réglementation en cours inversent cette tendance. La première priorité de l'Union tient désormais dans la régulation par les instances publiques, en imposant de nouvelles obligations à venir pour les systèmes de recommandation, mais aussi concernant la transparence et la marge d'action laissée aux utilisateurs finaux des services de ces grandes plateformes.

Les systèmes de recommandation étant constitués essentiellement d'algorithmes d'IA, il aurait pu être attendu du récent projet de règlement sur l'IA[265] en date d'avril 2021, que ce dernier fournisse des pistes d'encadrement. Publiée un an après le Livre blanc sur l'IA[266] de la Commission européenne, cette proposition définit les systèmes d'IA comme *« un logiciel* […] *qui peut, pour un ensemble donné d'objectifs définis par l'homme, générer des résultats tels que des contenus, des prédictions, des recommandations ou des décisions influençant les*

[263] POULLET (Y.), RUFFO DE CALABRE (M.-N.), « La régulation des réseaux sociaux », *op. cit.* note 90, p. 24.
[264] COMMISSION EUROPEENNE, *EU Code of Pratice on Disinformation, op. cit.* note 245.
[265] Proposition de Règlement du Parlement européen et du Conseil établissant des règles harmonisées concernant l'intelligence artificielle (législation sur l'intelligence artificielle) et modifiant certains actes législatifs de l'Union, COM/2021/206 final, 21 avril 2021, [en ligne], [consulté le 13 août 2021].
[266] COMMISSION EUROPEENNE, *Intelligence artificielle : une axée sur la confiance et l'excellence* [en ligne], COM(2020) 65 final, 19 février 2021, [consulté le 13 août 2021].

*environnements avec lesquels il interagit* » [267]. Si cette définition apparait très large, il est difficile de déterminer si les « *recommandations* » visent les systèmes de recommandation, ou plus simplement les algorithmes fournissant des propositions dans le domaine médical ou de la justice prédictive notamment. Selon Cécile Crichton, les systèmes de recommandation n'y figureraient pas[268]. Un constat similaire a été fait par la suite dans un avis du CEPD en juin 2021, reprochant par ailleurs l'exclusion des risques collectifs, et pour la société dans son ensemble[269]. Enfin, certaines interdictions au sens de cette proposition sont encore trop évasives, telles que l'interdiction de l'utilisation d'un système « *qui a recours à des techniques subliminales au-dessous du seuil de conscience d'une personne pour altérer substantiellement son comportement* »[270]. Selon le professeur de droit britannique Michael Veale, il peut être attendu dans les temps à venir que de nombreux lobbyistes tentent d'exclure explicitement les systèmes de recommandation[271]. Cette affirmation n'est pas sans rappeler la période de gestation du RGPD, ayant subit pas moins de 3 000 amendements[272]. L'incertitude est encore de mise s'agissant des effets de ce futur règlement sur les systèmes de recommandation, mais cette incertitude n'en est pas pour autant si dérangeante.

En effet, d'autres projets envisagent d'encadrer spécifiquement ces systèmes en imposant aux grandes plateformes de nouvelles obligations de contrôle et de transparence (Chapitre 1). Il s'agit là d'un progrès notable, compte tenu des insuffisances et inadaptations du droit contemporain expliquées précédemment. Il sera intéressant d'envisager par la suite d'autres mesures s'appliquant spécifiquement aux systèmes de recommandation (Chapitre 2), que ce soit par l'élaboration de nouveaux principes, d'une responsabilisation accrue des plateformes faisant usage de ces algorithmes, mais aussi de disposition extra-judiciaires pouvant accompagner l'effectivité de ces nouvelles mesures.

[267] Législation sur l'intelligence artificielle, art. 3. (1).
[268] CRICHTON (C.), « Projet de règlement sur l'IA (II) : une approche fondée sur les risques », *Dalloz actualité* [en ligne], 4 mai 2021, [consulté le 13 août 2021].
[269] CEDP, CONTR. EPD, *Joint Opinion 5/2021 on the proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act)* [en ligne], 18 juin 2021, pt. 17, [consulté le 13 août 2021].
[270] Législation sur l'intelligence artificielle, art. 5.
[271] HEAVEN (W. D.), « This has just become a big week for AI regulation », *MIT Technology Review* [*en ligne*], 21 avril 2021, [consulté le 13 août 2021].
[272] V. en ce sens : LOBBYPLAG, aperçu des 3132 amendements déposés sur le RGPD, [en ligne], [consulté le 14 août 2021].

# CHAPITRE 1 – L'EMERGENCE DE NOUVELLES OBLIGATIONS DE CONTROLE ET DE TRANSPARENCE

Le 15 décembre 2020, deux projets de règlement européen ont été déposés par l'Union européenne, la nouvelle législation sur les services numériques, le *Digital Services Act* (DSA)[273], et la législation sur les marchés numériques, le *Digital Market Act* (DMA)[274].

Le DSA vise à encadrer et imposer de nouvelles obligations aux grandes plateformes. Les apports de ces projets de règlements sont nombreux, et auront pour incidence d'apporter des éclaircissements sur l'usage des systèmes de recommandation, la publicité ciblée et la diffusion du contenu opéré par les grandes plateformes. Le projet de règlement DSA remplacera l'actuelle directive sur le commerce électronique[275] qui apparait aujourd'hui obsolète par rapport à l'évolution technologique des plateformes numériques. Cette directive transposée en France par la Loi pour la confiance dans l'économie numérique (LCEN)[276] en 2004, opérait une distinction entre un éditeur[277] de contenu, qui définit et contrôle les contenus publiés et en est par conséquent responsable, et un hébergeur[278], qui se contenterait de mettre à disposition passivement du contenu publié par d'autres, lui permettant de bénéficier d'un principe d'irresponsabilité[279]. Ce principe a été conservé par la nouvelle réglementation.

[273] Proposition de règlement du Parlement européen et du Conseil relatif à un marché intérieur des services numériques (Législation sur les services numériques) et modifiant la directive 2000/31/CE, COM/2020/825 final, [en ligne] [consulté le 6 août 2021].
[274] Proposition de règlement du Parlement européen et du Conseil relatif aux marchés contestables et équitables dans le secteur numérique (législation sur les marchés numériques), COM/2020/842 final, [en ligne] [consulté le 6 août 2021].
[275] 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 («*directive sur le commerce électronique*»), [en ligne] [consulté le 7 août 2021].
[276] Loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique, [en ligne] [consulté le 6 août 2021].
[277] Par son rôle actif, l'éditeur d'un service de communication au public en ligne est responsable du contenu qu'il diffuse, et est soumis à différentes obligations. V. en ce sens : LCEN, art. 6. III.
[278] LCEN, art. 6. I. 2., les hébergeurs se définissent comme étant « *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.* ».
[279] Par ce principe, l'hébergeur n'engagera sa responsabilité que s'il a connaissance d'un contenu litigieux manifestement illicite, et qu'il n'a pas réagi promptement pour retirer ce contenu. V. en ce sens : LCEN, art. 6. I. 2.

Cependant, comparativement aux années 2000, les plateformes jouent dorénavant un rôle fondamental dans la structuration des comportements politiques, commerciaux et sociaux. À l'aide de leurs méthodes de recommandation, de classification et de valorisation du contenu, les activités de ces plateformes sont aujourd'hui bien différentes[280]. Ce constat est sûrement à l'origine du fait que ce projet consacre (enfin), dans un texte réglementaire, les conséquences de ces systèmes. Ces derniers peuvent en effet « *avoir une incidence significative sur la capacité des bénéficiaires à récupérer les informations en ligne* », et jouent également « *un rôle important dans l'amplification de certains messages, la diffusion virale de l'information et la stimulation du comportement en ligne* »[281]. Le bilan global des nouvelles obligations issues de ce texte apparait protecteur pour les utilisateurs. Pour preuve, cette proposition a tellement effrayé Google, qu'un document interne à l'entreprise prévoyait de saboter le texte. Fort malheureusement pour Google, le document pernicieux a été dévoilé par la presse[282].

Le DMA quant à lui, a pour vocation principale d'améliorer l'équité entre les plateformes, en règlementant notamment les contrôleurs d'accès au marché, qualifiés de *Gatekeepers*[283]. Bien que le DMA apporte de nouvelles solutions intéressantes en matière de transparence et d'équité dans le référencement des produits, le DSA traite plus particulièrement la question des systèmes de recommandation et de leurs impacts sur les individus.

Il sera donc essentiellement question de traiter les apports à venir du DSA (Section 1), mais aussi, à partir des différentes critiques et recommandations ayant suivi la publication de ce projet, de constater de quelle manière la transparence et le contrôle de ces systèmes par les utilisateurs pourraient être élargis (Section 2).

[280] BRUNESSEN (B.), « Chronique Droit européen du numérique – La volonté de réguler les activités numériques », *RTD Eur.*, 2021, p. 160.
[281] DSA, cons. 62.
[282] VITARD (A.), « Google accusé de saboter le Digital Services Act, Sundar Pichai s'excuse », *L'usine digitale* [en ligne], 16 novembre 2020, [consulté le 8 aout 2021].
[283] Les contrôleurs d'accès sont qualifiés comme tel dès lors qu'ils remplissent trois critères : un poids important sur le marché intérieur, l'assurance d'un service de plateforme essentiel, et la jouissance d'une position solide et durable dans ses activités. V. en ce sens : DMA, art. 3.

## SECTION 1 – LES APPORTS DE LA LEGISLATION SUR LES SERVICES NUMERIQUES

La mise en place de ce projet a été appuyée par certaines évaluations de la proposition de règlement. Ces dernières ont été assorties d'une consultation publique des parties intéressées[284] et d'analyses d'impact[285] afin d'évaluer les conséquences de la mise en place de cette réglementation. La première idée venant à l'esprit face à ces différents travaux est la prise de conscience des régulateurs européens du danger de la manipulation des intérêts et de l'attention des individus par les algorithmes. En début 2020 déjà, une communication intitulée *Façonner l'avenir numérique de l'Europe* faisait le constat que « *Les citoyens ne se sentent plus en mesure de contrôler ce qu'il advient de leurs données personnelles et voient leur attention de plus en plus captée par des sollicitations artificielles. »*[286].

Le DSA a donc l'ambition de participer à un meilleur contrôle par les citoyens européens des outils proposés par les plateformes en ligne, d'autant plus qu'en matière de droits fondamentaux, il a été conclu que le règlement proposé permettra notamment de stimuler « *la liberté de recevoir des informations et d'avoir des opinions* », et « *renforcera les possibilités de recours des utilisateurs* »[287].

Les apports à venir du DSA pour les systèmes de recommandation pourraient finalement être répertoriés en deux idées principales. D'une part, une nouvelle logique d'évaluation des risques inhérents aux systèmes de recommandation est prévue (I). D'autre part, cette évaluation des risques s'accompagne d'un véritable impératif de transparence de ces systèmes (II).

# I – Une nouvelle logique d'évaluation des risques

Avant d'entrer dans les détails du contrôle de ces systèmes, il apparait important de souligner que cette règlementation propose la toute première définition spécifique aux systèmes de recommandation dans un texte juridique contraignant. Il aura donc été nécessaire d'attendre

[284] MAXIMIM (N.), « Plateformes : la Commission européenne a ouvert une consultation sur le Digital Services Act », *Dalloz IP/IT* [en ligne], 8 juin 2020, [consulté le 7 août 2021].
[285] COMMISSION EUROPEENNE, *analyse d'impact accompagnant la proposition de règlement sur les services numériques* [en ligne], SWD(2020) 348 final, 15 décembre 2020, [consulté le 7 août 2021].
[286] COMMISSION EUROPEENNE, *Façonner l'avenir numérique de l'Europe* [en ligne], communication de la Commission au Parlement européen, au Conseil, au Comité économique et social européen et au Comité des régions, COM(2020) 67 final, 19 février 2020, p. 1. [consulté le 7 août 2021].
[287] DSA, exposé des motifs.

jusqu'en 2021, pour considérer qu'un système de recommandation se définit comme « *un système entièrement ou partiellement automatisé utilisé par une plateforme en ligne pour suggérer dans son interface en ligne des informations spécifiques aux bénéficiaires du service, notamment à la suite d'une recherche lancée par le bénéficiaire ou en déterminant de toute autre manière l'ordre relatif d'importance des informations affichées* »[288].

Néanmoins, les obligations spécifiques aux systèmes visés par cette définition seront applicables uniquement pour certaines plateformes, désignées comme étant des *très grandes plateformes en ligne* (TGP). Seront qualifiées de TGP, les plateformes en ligne disposant d'un nombre d'utilisateurs européens mensuel de 45 millions[289]. Ce seuil de 45 millions d'utilisateurs correspond en réalité à 10% des résidents européens, et aura donc la particularité de s'ajuster afin de correspondre à ce taux dès lors qu'un changement démographique dans l'UE s'opère à hauteur de 5%.

Pour ces TGP, le projet de règlement envisage d'établir une évaluation des risques sur le fonctionnement et l'utilisation de leurs services. Cette évaluation comprend la diffusion de contenus illicites, tout effet négatif sur les droits fondamentaux (notamment sur la liberté d'expression et d'information), ainsi que les manipulations intentionnelles de leurs services avec des effets négatifs avérés sur la protection du discours civique, ou les processus électoraux par exemple[290].

La Commission européenne semble avoir tiré des leçons du manque d'efforts effectué par les plateformes en ligne[291], et de leur tendance à jouer sur les ambiguïtés notionnelles, à l'instar de Facebook qui ne publiait pas d'informations sur leurs algorithmes de recommandation[292]. C'est pourquoi il est explicitement mentionné que cette évaluation des risques tiendra compte de la manière dont « *leurs systèmes de modération des contenus, systèmes de recommandation et systèmes de sélection et d'affichage de la publicité* »[293] influence les risques précités, y compris

[288] DSA, art. 2. o.
[289] *Ibid*, art. 25. 1.
[290] *Ibid*, art. 26. 1.
[291] LE CALME (S.), « Commission européenne : Facebook, Google et Twitter ne respectent pas le code de conduite volontaire qu'ils ont signé pour combattre les fake news », *Developpez* [en ligne], 1 mars 2019, [consulté le 13 août 2021].
[292] CSA, *Lutte contre la diffusion de fausses informations sur les plateformes en ligne : bilan de l'application et de l'effectivité des mesures mises en œuvre par les opérateurs en 2019*, *op. cit.* note 249, p. 37.
[293] DSA, art. 26.

pour les risques de diffusion rapide et à grande échelle de contenus illicites, et d'informations incompatibles avec leurs conditions générales.

De grands espoirs se manifestent au travers de cette nouvelle obligation, car les données et études permettant d'évaluer juridiquement les risques de ces systèmes restaient jusqu'alors relativement rares. Cette évaluation comporte deux avantages non négligeables : d'une part, elle pourra pleinement rendre compte des risques inhérents aux systèmes de recommandation, là où l'analyse d'impact prévue par le RGPD[294] se focalisait certes sur les risques pour les droits et libertés des individus, mais ne permettait pas de viser explicitement les risques de manipulation de l'information, ou d'atteinte au droit à l'information. D'autre part, cela pourra permettre de faciliter le devoir d'atténuation des risques[295], qui est une nouvelle obligation prévue par le DSA.

Ce devoir d'atténuation des risques prévoit notamment d'adapter les processus décisionnels et caractéristiques des systèmes de recommandation en fonction des risques identifiés. Ce devoir d'atténuation pourrait donc permettre de limiter les effets négatifs déjà mentionnés de ces systèmes, comme le risque de dérive vers du contenu de plus en plus extrême par l'algorithme de YouTube par exemple[296].

Ces obligations d'évaluation et d'atténuation sont certes importantes, mais encore faut-il assurer un contrôle effectif du respect de ces obligations. Les précédentes réglementations en matière de diffusion du contenu en ligne souffraient par exemple d'un manque de contrôle des mesures effectivement mises en place par les grandes plateformes[297], et d'une absence de considération des systèmes de recommandation. Dorénavant, la nouvelle réglementation permettra selon l'Union européenne de renforcer ce contrôle par la mise en place d'inspections et d'audits des systèmes de modération des contenus, des systèmes de recommandation et de la publicité en ligne sur les très grandes plateformes[298].

[294] RGPD, art. 35.
[295] DSA, art. 27.
[296] SIX (N.), « L'algorithme de recommandation de YouTube critiqué pour sa mise en avant de contenus extrêmes », *op. cit.* note 53.
[297] CSA, « Le CSA expose sa vision d'une nouvelle régulation européenne », *11e réunion de l'ERGA* [en ligne] , 27 juin 2019, [consulté le 7 août 2021].
[298] DSA, 28.

Ces audits seront, à la différence de ce qui était prévu dans la logique d'autorégulation du RGPD, des audits externes devant remplir les conditions d'indépendance, d'expertise et d'objectivité prévues par le règlement[299]. Là où l'analyse d'impact du RGPD n'est soumise à aucune obligation de publication, ces audits seront contraignants et publiés. Naturellement, la comparaison entre ces deux types d'audit est limitée, puisque les obligations prévues par le RGPD ont un champ d'application très vaste. Cette problématique s'efface du fait que le nombre d'entités concernées par la qualification de TGP est beaucoup plus restreint, et permet d'appliquer un contrôle plus strict du respect des obligations de ces acteurs.

Certains auteurs s'étonnaient « *de la hardiesse du projet européen quand on sait que les plateformes visées sont largement américaines et que l'approche préventive d'évaluation, à peine esquissée dans le cadre du RGPD, restait purement interne à l'entreprise* »[300]. Il s'agit bel et bien d'une prise en main de l'Union européenne sur les conséquences de ces systèmes. Dans une optique de souveraineté numérique, il apparait nécessaire de réglementer afin de limiter les effets néfastes de ces outils que l'Union européenne n'est pas encore en mesure de reproduire du fait de son retard technologique[301].

Deux autres obligations permettent d'encourager le respect des obligations, et de faciliter l'évaluation des risques systémiques de ces algorithmes de recommandation. En premier lieu, le respect des obligations sera assuré par la désignation d'un ou plusieurs responsables de conformité[302]. En second lieu, les très grandes plateformes devront fournir aux États-membres ou à la Commission un accès aux données nécessaires qui permettront à des chercheurs agréés d'enquêter sur les risques systémiques des algorithmes de recommandation notamment[303].

Cette dernière disposition est particulièrement importante du fait que la recherche scientifique permet de demander des comptes aux acteurs puissants, et est par conséquent précieuse dans une société démocratique[304]. En effet, la protection des données ne doit pas être détournée afin de permettre à ces acteurs d'échapper à leurs responsabilités. Cette recherche, sous réserve de

---

[299] *Ibid*.
[300] POULLET (Y.), RUFFO DE CALABRE (M.-N.), « La régulation des réseaux sociaux », *op. cit.* note 90, p. 26.
[301] G'SELL (F.), « qu'est-ce que la souveraineté numérique ? », *Chaire Digital, Gouvernance et Souveraineté* [en ligne] , 9 juillet 2020, [consulté le 8 août 2021].
[302] DSA, art. 32.
[303] *Ibid*,. art. 31.
[304] CONTROLEUR EUROPEEN DE LA PROTECTION DES DONNEES, *Avis n° 01/2021 concernant la proposition de législation sur les services numériques* [en ligne] , 10 février 2021, p. 20. [consulté le 8 août 2021].

respecter le principe de proportionnalité et de mettre en place des garanties appropriées (conformément aux principes du RGPD concernant le traitement à des fins de recherche scientifique[305]), devrait permettre d'accéder aux *API*[306] nécessaires et aux autres données afin de récolter davantage d'informations sur les systèmes de recommandation de ces plateformes[307].

Bien qu'un contrôle renforcé de ces plateformes et de l'organisation de leur contenu soit prévu, il est important de souligner que le contrôle par les plateformes elles-mêmes du contenu publié reste relatif, le règlement préservant l'interdiction générale d'obligation de surveillance des plateformes[308]. Cette règle – qui fait écho à la censure quasi-intégrale par le Conseil constitutionnel[309] de la loi Avia[310] – était déjà présente lors du régime de responsabilité initial des hébergeurs[311]. Il s'agit là d'un tout autre registre, touchant à la liberté d'expression des utilisateurs des plateformes en ligne. Cette limitation est justifiée par deux raisons : l'obligation générale de surveillance peut limiter la liberté d'expression ainsi que la liberté de recevoir des informations, et risque de faire peser une charge excessive et inutile sur les plateformes[312]. L'interdiction de la mise en place de cette obligation reste donc bienvenue, et permet plutôt de se concentrer sur le contrôle des modalités de hiérarchisation mises en place par les TGP.

Aux côtés de cette nouvelle logique d'évaluation des risques, figure un véritable impératif de transparence de ces systèmes de recommandation.

---

[305] RGPD, art. 89.

[306] L'interface de programmation d'applications, ou *Application Programming interface* (API), est une interface standardisée qui permet aux applications de communiquer et de fonctionner entre elles. L'accès à ces API permet notamment la compréhension des fonctionnalités utilisées par les plateformes. V. en ce sens : Wikipedia, « Interface de programmation », version du 18 août 2021, [en ligne], [consulté le 10 août 2021].

[307] V. en ce sens : CONTROLEUR EUROPEEN DE LA PROTECTION DES DONNEES, *A Preliminary Opinion on data protection and scientific research* [en ligne], 6 janvier 2020, p. 16, [consulté le 14 août 2021].

[308] DSA, art. 7.

[309] Cons. const., 18 juin 2020, n° 2020-801 DC.

[310] Loi n° 2020-766 du 24 juin 2020 visant à lutter contre les contenus haineux sur internet. Avant son entrée en vigueur, le texte avait pour ambition de créer un nouveau délit de non-retrait des contenus haineux dans de brefs délais.

[311] Cette obligation trouve sa source au sein de la Directive 2000/31/CE sur le commerce électronique, art. 15 : *« Les États membres ne doivent pas imposer aux prestataires* […] *une obligation générale de surveiller les informations qu'ils transmettent ou stockent, ou une obligation générale de rechercher activement des faits ou des circonstances révélant des activités illicites. ».*

[312] BRUNESSEN (B.), « Chronique Droit européen du numérique – La volonté de réguler les activités numériques », *op. cit.* note 280.

## II – Un impératif de transparence des systèmes de recommandation

Contrairement à l'image d'objectivité souvent associée à la plupart des outils technologiques, le code informatique d'un algorithme n'est pas neutre et objectif. Derrière l'application se trouve encore une base humaine. Certains auteurs poussent la réflexion plus loin, en assimilant le code informatique à un instrument de régulation des droits de l'utilisateur, susceptible de servir les intérêts de la personne ayant programmé ce code. Il en est le cas pour Lawrence Lessig, qui utilisait la formule « *Code is Law* » en guise d'ouverture du premier chapitre de son livre *Code : And Other Laws of Cyberspace*[313]. Cette logique est d'autant plus vraie lorsque les recommandations servent une économie de l'attention fonctionnant au détriment des utilisateurs.

En France, la volonté d'imposer une transparence aux plateformes en ligne a été introduite dans le Code de la consommation depuis la loi pour une République numérique : « *Tout opérateur de plateforme en ligne est tenu de délivrer au consommateur une information loyale, claire et transparente sur : (…) les modalités de référencement, de classement et de déréférencement des contenus, des biens ou des services auxquels ce service permet d'accéder.* »[314].

Cependant, force est de constater que ces exigences n'ont pas été suffisantes pour faire respecter le besoin de transparence concernant les algorithmes de recommandation. C'est la raison pour laquelle le DSA envisage sur le plan européen d'améliorer cette transparence.

Cet impératif de transparence se traduit principalement par la mise en place d'une nouvelle obligation à destination des utilisateurs. Cette obligation sera contenue dans un article spécifiquement prévu pour les systèmes de recommandation. Les TGP auront l'obligation dans leurs conditions générales d'établir « *de manière claire, accessible et aisément compréhensible, les principaux paramètres utilisés dans leurs systèmes de recommandation, ainsi que les options dont disposent les bénéficiaires du service pour modifier ou influencer ces principaux*

[313] LESSIG (L.), *Code : And Other Laws of Cyberspace, Version 2.0*, Basic Books, 2006, p.1.
[314] Code de la consommation, art. L117-2 II.

*paramètres qu'elles auraient rendus accessibles* »[315]. Parmi ces options, devra y figurer au minimum une option « *qui ne relève pas du profilage* »[316].

Cette dernière option peut être vue comme un début de basculement de la décision de profilage, dont l'évaluation de sa nécessité et des fondements était laissée à l'appréciation des responsables de traitement sous réserve de respecter (relativement) les dispositions générales du RGPD. La mise à disposition auprès des utilisateurs d'une option de configuration des recommandations sans profilage permettra de faciliter davantage la gestion de leur vie privée, et de fournir un outil supplémentaire pour atténuer l'impact de leurs *bulles de filtre* au quotidien.

Cette mesure donnant la possibilité à échapper au profilage accompagne visiblement le durcissement des possibilités de ciblage publicitaire des individus, initié notamment par les lignes directrices de la CNIL sur les cookies. Certains envisagent la fin des cookies[317], avec les initiatives de plus en plus nombreuses telles que le blocage de cookies tiers sur le navigateur Firefox, ou la fin annoncée par Google des cookies tiers sur leur navigateur d'ici 2022… repoussé en 2023[318].

Cependant, cette option permettant de ne pas faire l'objet de recommandations sur le profilage sera-t-elle suffisamment mise en avant par les plateformes ? L'utilité de cette mesure règlementaire sera-t-elle suffisamment communiquée aux utilisateurs ? Il est difficile d'anticiper les effets d'un texte dont l'efficacité dépend finalement beaucoup de la diligence des plateformes. Ces nouvelles dispositions doivent sans surprise s'accompagner de mesures dépassant le champ d'application du Droit, mesures qui seront examinées plus en profondeur au sein du dernier Chapitre du présent mémoire. En tout état de cause, le manquement à ces obligations pourra notamment aboutir à une amende pouvant atteindre 6% du chiffre d'affaires mondial[319], sanction que la Commission européenne pourra infliger d'elle-même dans le cas des TGP.

[315] DSA, art. 29.
[316] *Ibid.*
[317] ARCELIN (L.), FOURGOUX (J.-L.), *Droit du marché numérique*, LGDJ, 2021, p. 239.
[318] TERRASSON (B.), « Google repousse la fin des cookies tiers à 2023 », *SiècleDigital* [en ligne], 25 juin 2021, [consulté le 17 août 2021].
[319] DSA, art. 59.

Les algorithmes de recommandation favorisent la visibilité de la fausse information et du contenu clivant dans le but de générer toujours plus d'interaction et de *« temps de cerveau humain disponible* »[320] pour la publicité. Il serait donc pernicieux de ne pas évoquer les mesures mises en place pour encadrer ces publicités.

De la même manière que la constitution d'un registre des activités de traitement (non publié) est prévue par le RGPD[321], cette fois-ci, un registre publié aux utilisateurs des plateformes est envisagé afin de fournir les informations nécessaires à ces derniers[322]. Un « listing » comparable a été pensé par la règlementation, obligeant les TGP à fournir des informations sur le contenu de la publicité, les personnes physiques ou morales pour le compte de laquelle la publicité est affichée, la période d'affichage, le groupe visé et le nombre de bénéficiaires atteint.

Il était admis que la transparence en matière de publicité n'était clairement pas atteinte par les dispositions de droit contemporain. Par exemple, la publicité affichée sur les réseaux sociaux Facebook et Instagram, dispose d'une option permettant de comprendre pourquoi l'utilisateur voit cette publicité. Certaines informations sur la visée géographique, la tranche d'âge ou les centres d'intérêts sont affichés à l'utilisateur. En revanche, comment savoir la raison pour laquelle cette publicité en particulier a été affichée sur le fil d'actualité de l'utilisateur ? Quel mode de sélection a été déployé afin d'afficher ce contenu publicitaire en particulier, plutôt que l'une des quelques milliers d'autres publicités utilisant les mêmes critères de ciblage ? Ce projet ne répond pas encore à cette problématique.

Enfin, pour renforcer la transparence de ces mesures, une obligation de transmettre un rapport rendant compte des résultats de l'évaluation des risques, ainsi que les mesures d'atténuations et audits réalisés tous les 6 mois est envisagée[323]. Néanmoins, les TGP auront la possibilité de retirer certaines informations lorsqu'elles considèrent ces informations comme susceptibles de compromettre la sécurité de son service ou encore lorsqu'il s'agit d'informations confidentielles pour la plateforme.

---

[320] Il s'agit là d'une expression popularisée par Patrick Le lay en 2004 pour désigner la capacité des marques publicitaires à influencer la perception humain.. V. en ce sens : BARTHELEMY (P.), « Comment les grandes marques influent sur nos cerveaux », *Le monde* [en ligne], 16 juin 2013, [consulté le 15 août 2021].
[321] RGPD, art. 30.
[322] DSA, art. 30
[323] *Ibid*., art. 33.

Il faut ici prendre en compte le fait que les algorithmes bénéficient d'une protection par le secret des affaires, protégeant essentiellement *« une information connue par un nombre restreint de personnes, qui a une valeur commerciale, effective ou potentielle, en raison de son caractère secret et qui fait l'objet de mesures de protection raisonnables pour conserver ce caractère secret* »[324]. Ce secret des affaires bénéficie de quelques protections par le droit européen, pénal, et par l'interdiction de la concurrence déloyale, mais reste moins protecteur que la propriété intellectuelle, qui ne permet cependant pas de protéger les fonctionnalités d'un algorithme, étant établi par la CJUE que « *la fonctionnalité d'un programme d'ordinateur* » ne constitue pas *« une forme d'expression de ce programme et ne sont, à ce titre, protégés par le droit d'auteur* »[325].

Le conflit entre la transparence et le secret des affaires n'est pas nouveau, il sera tout état de cause intéressant de constater dans quelle mesure cette protection – légitime pour sauvegarder l'intérêt économique des plateformes – sera interprétée par les plateformes s'agissant des informations à obstruer ou non sur le fonctionnement de leurs algorithmes de recommandation.

Bien que cette réglementation constitue un premier pas vers un véritable encadrement juridique des systèmes de recommandation, certaines améliorations pourraient être effectuées principalement sur le contrôle et l'évaluation des systèmes de recommandation, et sur leur transparence.

[324] MARTY (F.), « La protection des algorithmes par le secret des affaires. Entre risques de faux négatifs et risques de faux positifs », *RIDE* [en ligne], 2019/2 (t. XXXIII), pp. 211-237, [consulté le 15 août 2021].
[325] CJUE, 2 mai 2012, *SAS Institute Inc. v. World Programming Ltd*., aff. C-406/10, pt. 46.

## SECTION 2 – VERS L'ELARGISSEMENT DES OBLIGATIONS IMPOSEES AUX TRES GRANDES PLATEFORMES

Cette nouvelle législation sur les services numériques envisage donc d'imposer de véritables obligations aux TGP faisant usage de systèmes de recommandation. Cependant, certains points d'amélioration de cette règlementation pourraient être proposés. À ce titre, plusieurs acteurs se sont mobilisés afin de proposer une amélioration de celles-ci. Il sera donc vu qu'un élargissement des obligations imposées aux TGP pourrait être envisagé (I). Cet élargissement des obligations, pourrait tout aussi bien être accompagné de nouvelles possibilités de prise en main des systèmes de recommandation par les utilisateurs (II).

### I - L'élargissement des obligations imposées aux très grandes plateformes en matière de système de recommandation

Un premier point d'élargissement pourrait être défendu concernant l'évaluation des risques systémiques des algorithmes de recommandation. À ce sujet le Sénat, dans son avis du 18 mars 2021 sur la désinformation en ligne et les atteintes aux processus électoraux[326] s'est exprimé sur la possibilité d'améliorer ce dispositif. En effet, le Sénat est resté dubitatif sur la limitation de l'évaluation des risques de ces systèmes aux cas de manipulation « *intentionnelle* » prévue par l'article 26 du DSA. Ce dernier encourageait à prendre plus particulièrement en compte les effets négatifs « *pouvant découler du fonctionnement même du modèle économique de ces plateformes, reposant sur la monétisation des contenus* »[327]. En somme, le Sénat invite à considérer dans l'évaluation de ces systèmes, la possibilité d'influencer de façon néfaste le contenu des utilisateurs, non pas dans une logique de manipulation étatique ou idéologique consciente, mais tout simplement par la logique issue de l'économie de l'attention.

Toujours dans l'évaluation proposée par l'article 26 du projet de règlement, d'autres auteurs ont considéré que le règlement devrait aussi intégrer plus explicitement dans ses critères d'évaluation, les modalités de classement et de référencement utilisées par les plateformes, puisque ces critères ont aussi des effets systémiques notables[328]. L'absence de ces mentions

[326] SENAT, *Avis politique sur la désinformation en ligne et les atteintes aux processus électoraux*, *op. cit.* note 142.
[327] *Ibid., cons. 77.*
[328] CRICHTON (C.), « Le Digital Service Act, un cadre européen pour la fourniture de services en ligne », *Dalloz actualité IP/IT* [en ligne], 8 janvier 2021, [consulté le 9 août 2021].

s'accompagne d'une autre déception : le projet ne concerne pas l'activité des moteurs de recherche. Cela est regrettable, en considérant l'importance de leur rôle en matière d'accessibilité du contenu pour les utilisateurs et de leurs modes d'ordonnancement des résultats de recherche. Les obligations imposées pour le contrôle et la transparence des algorithmes auraient pu être mises en place pour les moteurs de recherche.

Du fait de l'impact sur le débat public de certaines plateformes, des effets de réseaux massifs, et de l'activité exercée, certaines plateformes pourraient aussi comporter un risque, sans pour autant entrer dans la catégorie initialement prévue des TGP. À ce titre, le Sénat envisageait d'élargir la portée des mesures d'atténuation des risques au-delà des très grandes plateformes, afin de s'intéresser aux risques réels de certaines plateformes pouvant passer entre les mailles du filet de la nouvelle règlementation[329].

Bien que l'extension du contrôle de ces systèmes puisse être envisagée, la transparence est tout aussi importante pour une utilisation plus saine de ces systèmes. Insistant sur la nécessité de minimiser l'impact des *bulles de filtre* et *chambres d'écho*, le Sénat est revenu sur les apports en matière de transparence des systèmes de recommandation contenus au sein de l'article 29 du DSA. En plus de cet article prévoyant que les utilisateurs aient au minimum la possibilité de recourir à un système de recommandation qui ne relève pas du profilage, un système de consentement préalable (*opt-in)* pourrait être mis en place[330]. Tout comme la prospection commerciale à destination des consommateurs est soumise à leur consentement préalable[331], les systèmes de recommandation pourraient tout simplement être fixés par défaut sur l'option n'étant pas basée sur le profilage, ce qui impliquerait une action positive de l'utilisateur s'il souhaite en bénéficier. Cette proposition, directement tirée d'un avis du Contrôleur européen de la protection des données en date de février 2021[332], aurait un grand intérêt à être appliquée.

Malgré le consentement des utilisateurs aux conditions générales d'utilisation, il a bien été montré que son caractère libre et éclairé n'était pas réellement présent lors de l'utilisation de ces services. Une protection par défaut permettrait donc d'éviter l'acceptation d'une

[329] SENAT, *Avis politique sur la désinformation en ligne et les atteintes aux processus électoraux, op. cit* note 142., *cons. 78.*
[330] *Ibid*., cons. 87.
[331] Code des postes et des communications électroniques, art. L34-5.
[332] CONTROLEUR EUROPEEN DE LA PROTECTION DES DONNEES, *Avis n° 01/2021 concernant la proposition de législation sur les services numériques, op. cit.* note 304, p. 20.

fonctionnalité algorithmique dont les effets pourraient ne pas être suffisamment considérés par les utilisateurs. De plus, une désactivation par défaut du profilage serait plus simplement protectrice à l'égard des individus présentant des difficultés à maitriser les outils technologiques, difficultés qui restent fréquentes actuellement.

Effectivement selon un rapport d'information du Sénat, 17% des français seraient encore en situation *d'illectronisme*[333]. Ce néologisme, se définissant comme « *l'état d'une personne qui ne maîtrise pas les compétences nécessaires à l'utilisation et à la création des ressources numériques* »[334], implique une exclusion par l'absence d'utilisation de matériel numérique certes, mais fait aussi référence à un manque de compétence dans l'utilisation de ces outils. Bien que de nombreux utilisateurs soient à l'aise avec l'utilisation des réseaux sociaux et des grandes plateformes, il n'y a pas forcément de corrélation entre la consommation quotidienne de contenu disponible sur une plateforme, et la compréhension des mécanismes de fonctionnement de celle-ci. Par conséquent, cet *illectronisme* n'épargne pas les plus jeunes générations pour autant[335].

En supplément de nouvelles possibilités de paramétrage non basées sur le profilage, la transparence sur le fonctionnement des systèmes de recommandation devrait être elle-aussi améliorée. Bien que le DSA prévoit une information sur ces systèmes présentée de manière claire, accessible et aisément compréhensible, le Contrôleur européen de la protection des données fait un constat tout à fait révolutionnaire : « *les conditions générales sont généralement des documents longs.* »[336].

Effectivement, il apparait difficile d'imaginer qu'un utilisateur considéré comme « *illectronique* » parvienne sans difficulté à comprendre le fonctionnement des algorithmes de recommandation d'une plateforme, d'autant plus si les conditions générales – comme il en est souvent le cas pour les très grandes plateformes – fournissent des informations sur de nombreux services connexes en parallèle[337]. Le Contrôleur européen de la protection des données

[333] SENAT, *L'illectronisme ne disparaîtra pas d'un coup de tablette magique !* [en ligne], rapport du Sénat pour la mission d'information sur l'inclusion numérique, 17 septembre 2020, [consulté le 9 août 2021].
[334] Dictionnaire Larousse en ligne, « illectronisme », [en ligne], [consulté le 9 août 2021].
[335] TELLIER (M.), « La fracture numérique n'épargne pas les jeunes », *France culture* [en ligne], 31 mai 2020, [consulté le 9 août 2021].
[336] CONTROLEUR EUROPEEN DE LA PROTECTION DES DONNEES, *Avis n° 01/2021 concernant la proposition de législation sur les services numériques, op. cit.* note 304, p. 20.
[337] Google compte actuellement plus 220 produits et services différents, dont les politiques de confidentialité et conditions générales se rejoignent parmi de nombreux onglets présentant dans l'ensemble une certaine complexité.

préconise donc que les informations concernant « *le rôle et le fonctionnement des systèmes de recommandation soient présentées séparément, d'une manière aisément accessible, claire pour les utilisateurs moyens et concise* »[338].

De manière plus générale, que ce soit pour les systèmes de recommandation ou pour les autres systèmes faisant usage de l'IA, les juristes mettent en avant depuis plusieurs années le rôle de transparence et de l'évaluation des risques au service d'un consentement renforcé[339]. Ensemble, ces dispositions renforceraient l'autodétermination des individus, un principe qui sera explicité au sein du prochain chapitre. En tout état de cause, malgré les efforts de transparence et de contrôle de ces systèmes, de nouvelles possibilités de prise en main pour l'utilisateur constitueraient aussi un accompagnement bénéfique pour la maitrise des systèmes de recommandation.

## II – De nouvelles possibilités de prise en main pour l'utilisateur

Malgré ces efforts de transparence, il est possible que les systèmes de recommandation soient sans friction pour l'utilisateur, quand bien-même leur impact serait significatif. Dès lors, le Contrôleur européen de la protection des données a établi une dernière liste d'améliorations possibles concernant le contrôle et la transparence des systèmes pour les individus[340]. Des plateformes plus transparentes incluraient de ce fait une indication bien visible du fait que la plateforme fait usage d'un système de recommandation tout en proposant des contrôles et options disponibles. Serait aussi disponible une information sur la personne responsable du système (afin de savoir si le système est géré par une autre entité que la plateforme), et la possibilité de visionner et supprimer à la convenance de l'utilisateur tous profils utilisés aux fins de curation[341] du contenu. Enfin, des options de personnalisation du système de recommandation pourraient être mises à disposition de l'utilisateur, en tenant compte de critères de base (sujets d'intérêts par exemple).

---

V. notamment : WEBRANKINFO, « Encyclopédie Google : produits, services, brevets… », [en ligne], [consulté le 8 août 2021].

[338] CONTROLEUR EUROPEEN DE LA PROTECTION DES DONNEES, *Avis n° 01/2021 concernant la proposition de législation sur les services numériques*, *op. cit.* note 304.

[339] CONSEIL DE L'EUROPE, *Intelligence artificielle et protection des données : enjeux et solutions possibles*, *op. cit.* note 191, p. 7.

[340] *Ibid.*, p. 21.

[341] V. pour plus de précisions : WIKIPEDIA, « Curation de contenu », version du 4 février 2021 [en ligne], [consulté le 8 août 2021], « *La curation de contenu est une pratique qui consiste à sélectionner, éditer et partager les contenus les plus pertinents du Web pour une requête ou un sujet donné* ».

À l'instar de l'avis du Contrôleur européen de la protection des données, la Commission nationale consultative des droits de l'homme (CNCDH) a formulé une préconisation invitant à la consécration d'un véritable droit au paramétrage effectif des contenus reçus et émis sur les TGP. Cette préconisation provient d'un avis relatif à la lutte contre la haine en ligne en date de juillet 2021, qui propose de revoir certaines dispositions du projet DSA[342]. En effet, la CNDCH est d'avis que le phénomène des *bulles de filtre* présente des dangers en matière d'autonomie de la personne, de liberté de conscience, de risque sur le pluralisme et de diversion d'opinion. Cela mérite donc d'aboutir à une approche prudente de la part des régulateurs, en conférant à l'utilisateur un pouvoir lui permettant de construire son propre espace et de le paramétrer selon ses intérêts et envies.[343] C'est une mesure qui apparait tout à fait essentiel dès lors que l'on considère que les intérêts de l'usager et de la société dans son ensemble devraient prévaloir sur les intérêts économiques et mécanismes de visibilité de la plateforme.

La CNCDH souligne l'importance d'un droit pour l'utilisateur de recevoir des contenus « neutres », à savoir des contenus qui ne seraient pas issus d'un système de recommandation comme l'article 29 du DSA l'envisageait. Dans cette continuité la création d'une option qui permettrait à l'utilisateur d'effectuer une recherche hors de ses intérêts habituels pourrait être établie à la manière de l'option de navigation privée présente sur les navigateurs web, mais appliquée aux plateformes telles que Facebook ou Instagram[344]. Un paradoxe propre aux utilisateurs de ces services numérique est aussi présent, il se caractérise par une volonté de prendre le contrôle de son espace numérique, tout en souhaitant y consacrer le temps le plus court possible. C'est pourquoi un niveau distinct de paramétrage, allant d'un premier niveau simple, à un niveau plus poussé pourrait être ajouté aux fonctionnalités des TGP.

Enfin, la CNCDH fait une proposition qui pourrait – et cela n'engage que l'avis de la présente recherche – s'avérer problématique. Cette dernière préconise l'ajout d'options sur les plateformes qui permettraient à l'utilisateur de décider par lui-même de favoriser certains contenus intéressants pour lui, et de refuser d'être exposé à d'autres contenus. Cependant, si cette option permettait de réduire l'effet de *bulle de filtre,* force est de constater que ce type

[342] CNDCH, *Avis relatif à la lutte contre la haine en ligne* [en ligne], (A - 2021 - 9), JORF n° 0170, 24 juillet 2021, [consulté le 14 août 2021].
[343] *Ibid*. pt. 82.
[344] *Ibid*. pt. 83.

d'option favoriserait d'autant plus le renforcement des *chambres d'écho*. Pour rappel, la *chambre d'écho* se caractérise davantage par un enfermement créé par l'utilisateur lui-même[345], contrairement à la *bulle de filtre* qui est formée par les règles insufflées aux algorithmes. Une telle disposition porterait donc probablement atteinte à la diversité des contenus proposés du propre fait de l'utilisateur.

Il apparait surprenant qu'une Commission rendant un avis destiné à lutter contre la haine en ligne, formule une proposition qui pourrait justement avoir l'effet inverse en pratique, et affecter en priorité les utilisateurs les plus susceptibles d'être sujets à un enfermement algorithmique propice à l'accès à du contenu favorisant l'émergence de la haine.

Un meilleur équilibre pourrait être atteint, non pas en excluant directement l'exposition à certains types de contenus, mais plutôt en permettant aux utilisateurs de gérer le niveau de recommandation propre à chaque type de contenu. Cette hypothèse, sera davantage détaillée lors du prochain chapitre.

Il a été vu que de nombreux changements sont à attendre grâce à ce nouveau règlement, bien que certaines améliorations mériteraient d'être mises en place concernant la transparence des systèmes de recommandation, et leur prise en main par les utilisateurs. Cette règlementation trouve cependant certaines limites, notamment du fait de son champ d'application. Cette limitation est bien entendu justifiée par la grande variété de dispositions déjà présentes au sein du DSA, et qui ne concernent pas forcément les algorithmes de recommandation. Il apparait donc pertinent d'envisager certaines dispositions plus spécifiques à ces systèmes, qui n'emporteraient pas les limitations inhérentes à la règlementation européenne.

[345] SUMPTER (D.), *Outnumbered : From Facebook and Google to fake news and filter-bubbles – the algorithms that control our lives, op. cit.* note 44.

# CHAPITRE 2 – L'ENCADREMENT DES SYSTEMES DE RECOMMANDATION : UNE APPROCHE PLURIDISCIPLINAIRE

Comme pour la plupart des branches inhérentes au droit du numérique, l'établissement d'un régime juridique est fondamental, mais nécessite en corollaire d'autres applications portées sur les technologies et nouveaux usages.

Au sein de ce dernier chapitre, le risque sera pris d'analyser de manière prospective quelles seraient les dispositions juridiques, mais aussi techniques, qui mériteraient une adaptation plus spécifique aux systèmes de recommandation. La finalité de cette analyse, est de proposer une alternative complémentaire aux règlementations européennes à venir afin de garantir au mieux que les systèmes de recommandation ne soient pas utilisés à des fins préjudiciables pour la société.

À ce titre, sera premièrement développé l'idée d'une consécration de principes juridiques au service d'une nouvelle responsabilisation des plateformes en ligne (Section 1). Le présent mémoire se conclura par une proposition qui pourrait théoriquement favoriser la reprise en main des utilisateurs de leur flux informationnel, une exigence qui devrait être considérée comme fondamentale aujourd'hui (Section 2).

## SECTION 1 – LA CONSECRATION DE PRINCIPES JURIDIQUES AU SERVICE D'UNE NOUVELLE RESPONSABILISATION DES PLATEFORMES EN LIGNE

En premier jalon d'une règlementation plus spécifique aux systèmes de recommandation, l'établissement de droits plus transversaux permettant d'assurer une protection élargie des utilisateurs devrait être mise en place. C'est en ce sens qu'il sera développé l'idée d'un droit au contrôle du flux informationnel, comme dérivé du droit à l'autodéterminée informationnelle (I). Enfin, le respect effectif de ce droit doit nécessairement s'accompagner d'une nouvelle forme de responsabilisation des plateformes (II).

### I – Pour un droit au contrôle du flux informationnel comme dérivé du droit à l'autodétermination informationnelle

Compter sur la mise en place d'une réglementation européenne afin d'encadrer les effets néfastes des systèmes de recommandation est un point de départ satisfaisant, mais pas optimal. Le numérique est un enjeu international, il ne devrait pas se circonscrire à l'Europe, bien que l'établissement de normes à cette échelle nécessite une coopération effective entre les États. Tout du moins à l'échelle européenne, le DSA mériterait d'être accompagné par l'élaboration de véritables principes juridiques s'exonérant de la contrainte d'un champ d'application restreint.

L'autodétermination informationnelle peut se définir comme la possibilité pour les individus de décider librement du devenir des informations numériques les concernant. Ce droit a été consacré pour la première fois par la Cour constitutionnelle allemande le 15 décembre 1983[346]. Ce droit, au-delà des DACP au sens strict, porte plus largement sur l'identité numérique des individus, formée par l'ensemble des traces laissées par son activité numérique.

L'exploitation de toutes ces données par des croisements, des prédictions, ou encore par la valorisation du surplus comportemental des individus en leur suggérant du contenu taillé sur mesure, justifie l'émergence progressive d'un tel concept. Dès lors, pourrait-il être considéré

[346] Bundesverfassungsgerichts 65,1, *Volkszählung*, 15 décembre 1983.

que l'exploitation des données aux fins de recommandations, puisse justifier l'existence d'un droit dérivé à l'autodétermination informationnelle ?

Il conviendra d'expliciter les contours et délimitation de ce droit à l'autodétermination informationnelle, afin de justifier en quoi la création d'un principe juridique transversal aux systèmes de recommandation serait utile.

Tout d'abord, ce droit à l'autodétermination informationnelle ne se résume pas à la protection de la vie privée, ni aux garanties du droit à la protection des données personnelles. Dans un article de 2020, Pauline Türk défend cette conception extensive du droit à l'autodétermination informationnelle de la manière suivante :

« *À l'heure où la « fondamentalisation » de certains droits du numérique est à l'étude, on peut considérer que, au regard de ses fondements et de sa portée, le droit à l'autodétermination informationnelle se distingue d'autres concepts et droits numériques émergents, dont il pourrait être un principe structurant, un socle ou un droit matriciel, justifiant de lui reconnaître une valeur juridique plus importante.* »[347]

Initialement, ce droit se rattache aux droits de la personnalité. En effet, la Cour constitutionnelle allemande fonde cette création prétorienne sur plusieurs dispositions de la Loi fondamentale allemande[348], notamment son article 2, consacrant le droit de chacun au libre épanouissement de sa personnalité. Les contours de ce droit ne se limitent pas à la protection des individus face aux plateformes et autres acteurs du numérique, il dispose aussi d'un caractère actif, induisant une capacité des individus à décider de l'utilisation de leurs données.

De ce droit à l'autodétermination informationnelle découlerait finalement les autres « droits dérivés », beaucoup plus concrets, qui permettent l'accès, la rectification, l'effacement, le déréférencement, et bien d'autres applications mises en place par les règlementations européennes et la jurisprudence. Somme toute, il pourrait être la « *matrice* », le véritable principe directeur, de la création de nouveaux droits émergents du numérique[349].

---

[347] TÜRK (P.), « L'autodétermination informationnelle : un droit fondamental émergent ? », *Dalloz IP/IT*, 2020, p. 616.
[348] Loi fondamentale pour la République fédérale d'Allemagne du 23 mai 1949, [en ligne], [consulté le 15 août 2021].
[349] TÜRK (P.), « L'autodétermination informationnelle : un droit fondamental émergent ? », *op. cit.* note 347.

En attente d'une véritable consécration sur le plan européen, le RGPD reconnait en filigrane ce principe qui figure selon Carine Copain-Héritier parmi les grands principes sous-jacents du RGPD[350]. La France aussi s'est rapprochée de ce droit une première fois dans une étude du Conseil d'État intitulée *Le numérique et les droits fondamentaux* en reconnaissant un « *droit personnel à l'autodétermination informationnelle* »[351], concept qui sera enfin consacré (de manière restrictive aux DACP) par la modification de la Loi informatique et liberté opérée par la loi pour une république numérique. Ainsi depuis 2016, « *toute personne dispose du droit de décider et de contrôler les usages qui sont faits des données à caractère personnel la concernant* »[352]. À son tour, l'Assemblée nationale n'a pas manqué de manifester son intérêt pour ce droit à l'occasion d'un procès fictif censé se situer en 2028[353], estimant l'autodétermination informationnelle comme une liberté fondamentale se déduisant de la dignité humaine.

Les problématiques inhérentes aux systèmes de recommandation sont difficiles à classifier au sein des typologies contemporaines, tant ces problématiques se situent dans un interstice entre les atteintes et risques pour les droits fondamentaux, la protection des données, le droit électoral et des médias, l'encadrement de l'IA et de l'économie des plateformes. Il pourrait dès lors être élaboré un principe plus général qui ne serait guère tributaire d'une règlementation telle que le DSA, au champ d'application qui pourrait s'avérer avec le temps trop restrictif.

La mise en place d'un véritable droit au contrôle du flux informationnel pourrait donc s'intégrer au sein de la matrice du droit à l'autodétermination informationnelle, à l'instar des autres créations juridiques et prétoriennes connues à ce jour.

Ce droit au contrôle du flux informationnel pourrait ainsi se définir comme étant la capacité pour tout individu à décider librement de l'organisation du flux informationnel constituant son espace numérique.

---

[350] COPAIN-HERITIER (C.), « Le cadre européen de la protection des données : entre forces et faiblesses intrinsèques », *Rev. UE*, 2021, p. 163.
[351] CONSEIL D'ÉTAT, *Le numérique et les droits fondamentaux* [en ligne], 9 septembre 2014, [consulté le 15 août 2021].
[352] LIL., art. 1.
[353] PREVOST (S.), « 2028 : procès du ranking social », *Dalloz actualité* [en ligne], 13 janvier 2020, [consulté le 15 août 2021].

Ce droit, tout comme l'autodétermination informationnelle, aurait vocation à s'appliquer aux systèmes d'IA. C'est ce que retenait le *Rapport sur l'intelligence artificielle* de la Convention 108 sur le principe d'autodétermination, qui considérait que ce concept pouvait être applicable au sens large pour faire référence à la « *liberté de choix concernant l'usage de l'intelligence artificielle et au droit à une version « non intelligente » de biens et services intégrant des technologies d'IA* »[354]. Cette volonté se retranscrit visiblement dans la mise en place par le DSA d'une possibilité d'utilisation des services dotés de systèmes de recommandation sans avoir recours à un profilage des utilisateurs[355].

Serait aussi considérée comme une première application concrète de ce droit l'émergence des nouvelles obligations précitées de transparence et de contrôle, ainsi que les fonctionnalités permettant la prise en main de l'utilisateur des systèmes de recommandation. Il ne s'agit pas ici de simplement abstraire des dispositions prévues par la règlementation européenne, mais plutôt de prévoir le risque que les dispositions européennes présentent leurs limites. En effet, l'application des dispositions spécifiques aux systèmes de recommandation étant circonscrite à un minimum de 10% d'utilisateurs européens mensuels[356], plusieurs cas de figure problématiques pourraient se présenter.

En premier lieu, une plateforme agissant uniquement à un niveau national, pourrait utiliser des algorithmes de recommandation pouvant s'avérer collectivement préjudiciables sans pour autant que les garanties spécifiques du DSA en matière de contrôle et de transparence puissent être mises en place, faute d'atteindre le nombre suffisant de 45 millions d'utilisateurs mensuels. Le caractère restrictif de la qualification de TGP est compréhensible du fait que le DSA envisage de nombreuses autres obligations relativement lourdes que celles spécifiques aux algorithmes de recommandation, mais gagnerait à s'articuler avec ce droit au contrôle du flux informationnel afin prévenir des risques inhérents à de potentiels services (présents ou à venir) qui pourraient se situer à un niveau plus restreint.

En second lieu, bien que les GAFAM soient implicitement la première cible de ces obligations, le phénomène de *balkanisation d'internet* ne doit pas être écarté. Ce phénomène, décrit comme

[354] CONSEIL DE L'EUROPE, *Intelligence artificielle et protection des données : enjeux et solutions possibles, op. cit.* note 191, p. 8.
[355] DSA, art. 29.
[356] DSA, art. 26.

une tendance d'internet à se diviser en raison de divers facteurs, qui peuvent être technologiques, politiques, commerciaux, ou simplement issus d'intérêts nationaux divergents, a été popularisé lors de la mise en place du « *Grand pare-feu de Chine* »[357], et réactualisé depuis l'adoption par la Russie en 2019 d'une loi[358] permettant au pays de créer une version russe du *Domaine Name Server*, et de couper son réseau. Il est tout à fait probable, sans imaginer de mesures aussi drastiques, que ce phénomène s'amplifie compte tenu de la volonté des pays européens de tendre vers une véritable souveraineté numérique, qui impliquera sûrement de développer ses propres outils, voir ses propres plateformes ou réseaux de discussion et d'actualité hébergeant du contenu classifié par des algorithmes de recommandation. La fragmentation de ces services diminuerait par conséquent les exigences de transparence en l'absence de qualification de TGP. Il en découlerait une obsolescence des règlementations qui, à moins de subir une adaptation, ne permettraient pas une réduction effective des effets néfastes des *bulles de filtre* et *chambres d'écho*, de potentielles désinformations ou recommandations nuisibles dans l'ensemble.

Ce droit au contrôle du flux informationnel, tout comme l'autodétermination informationnelle, aurait vocation à s'appliquer aux systèmes d'IA. Le *Rapport sur l'intelligence artificielle* de la Convention 108, considérait que l'autodétermination informationnelle déjà, pouvait être applicable au sens large pour faire référence à la « *liberté de choix concernant l'usage de l'intelligence artificielle et au droit à une version « non intelligente » de biens et services intégrant des technologies d'IA* »[359]. Cette volonté se retranscrit visiblement dans la mise en place par le DSA d'une possibilité d'utilisation des services dotés de systèmes de recommandation sans avoir recours à un profilage des utilisateurs[360].

Naturellement, l'établissement d'un principe juridique transversal nécessite en corollaire une responsabilisation des acteurs concernés.

---

[357] Illustration la plus connue d'une souveraineté numérique, le « *Grand pare-feu de Chine* » permet de bloquer le contenu indésirable aux yeux du gouvernement chinois. V. en ce sens : CREEMERS (R.). « Comment la Chine projette de devenir une cyber-puissance », *Hérodote* [en ligne], vol. 177-178, n° 2-3, 2020, pp. 297-311, [consulté le 15 août 2021].

[358] VITKINE (B.), « La Russie en quête de « souveraineté » sur Internet », *Le monde* [en ligne], 7 avril 2021, [consulté le 15 août 2021].

[359] CONSEIL DE L'EUROPE, *Intelligence artificielle et protection des données : enjeux et solutions possibles*, *op. cit.* note 191, p. 8.

[360] DSA, art. 29.

## II – Pour un développement de la responsabilisation des acteurs de la recommandation de contenus

Cette nouvelle forme de responsabilisation se justifierait, comme il a été vu précédemment, par les éventuelles limites de la règlementation à venir. Si une responsabilité devait être engagée, cette dernière devrait davantage être basée sur le risque de préjudice (individuel comme collectif dans le contexte d'une manipulation des recommandations), plutôt que sur la taille d'une plateforme. Il n'est pas à exclure qu'une petite plateforme en ligne s'adonne par la suite à certaines pratiques de référencement dont les règles spécifiques de ses algorithmes permettent de manipuler subtilement l'opinion publique, ou de maximiser des effets de bulle de filtre et de chambre d'écho pour certaines finalités politiques, ou simplement économiques.

Cependant, quel champ d'application, et quel fondement justifierait cette responsabilité ?

Concernant le champ d'application, il n'est pas nécessaire de réinventer la roue. La dichotomie établie entre le statut d'éditeur et d'hébergeur initiée par la directive sur le Commerce électronique pourrait suffire[361]. En effet, les plateformes ayant recours à des algorithmes de recommandation ont généralement en pratique le statut d'hébergeur, du fait que la masse de contenu présent nécessite un tri dans un fil d'actualité quelconque.

De ce fait, les plateformes bénéficient du principe d'irresponsabilité de l'hébergeur, lorsque le contenu publié sur leur plateforme n'est pas à leur initiative, à l'exception de la présence d'un contenu manifestement illicite dont ils ont eu effectivement connaissance et pour lequel ils n'ont pas agi promptement pour le retirer[362]. Ils disposent du statut d'éditeur dès lors qu'ils détiennent un rôle actif vis-à-vis du contenu publié, les rendant ainsi responsables de ce contenu et tributaires d'obligations imposées par le LCEN[363]. Néanmoins, bien que le champ d'application large du statut d'hébergeur puisse s'appliquer, la responsabilité des plateformes faisant un usage préjudiciable de leurs systèmes de recommandation ne peut pas se calquer sur l'appréciation de cette responsabilité, et nécessite une adaptation.

[361] Directive du 8 juin 2000 sur le commerce électronique, *op. cit.* note 275.
[362] LCEN, art. 6. I. 2.
[363] LCEN, art. 6. III.

En effet, l'appréciation de la responsabilité de l'hébergeur n'est pas une base satisfaisante, puisque cette responsabilité se limite à la caractérisation d'un contenu manifestement illicite. Au demeurant, cette qualification sera appréciée en France au cas par cas par la jurisprudence, par exemple par un contenu proposant des services illicites sur un territoire national et visant celui-ci[364], ou encore le cumul d'injures à l'encontre d'une personne[365] (sans considérer qu'il est nécessaire que le contenu soit « certainement » illicite, il doit uniquement l'être « manifestement »[366]).

Ainsi, il n'est pas réellement question de viser le contenu publié sur une plateforme. Le contenu préjudiciable peut généralement ne pas revêtir la qualification restrictive du contenu manifestement illicite, et il n'y aurait donc pas besoin de détailler les exigences du caractère prompt du retrait[367]. Même si ce contenu pourrait théoriquement être l'une des composantes d'un plus grand préjudice collectif, il ne serait pas judicieux de viser le contenu en question, ni l'auteur de ce dernier pour des raisons évidentes de liberté d'expression et de protection contre les possibilités de censure.

Si la plateforme n'est pas responsable *a priori* du contenu publié, et que ce contenu n'a pas vocation à être supprimé s'il n'est pas manifestement illicite, il s'agirait plutôt de viser les règles de l'algorithme de recommandation abusant de la logique propre à l'économie de l'attention, en priorisant le contenu excessivement clivant, ou en enfermant les individus dans des recommandations beaucoup trop personnalisées, dans un objectif de stimulation de l'interaction et de maintien excessif de l'attention.

Puisque l'atteinte opérée par ces systèmes résulte plus d'une atteinte collective aux droits fondamentaux des individus précités, il parait compliqué qu'un utilisateur intente une action telle qu'imaginée par la responsabilité civile pour l'IA, devant démontrer un lien fait générateur et un préjudice[368]. D'autant plus que le droit de l'IA est encore en construction actuellement, et que les questions de responsabilité en matière de voiture autonome par exemple, ne sont pas

[364] TGI Versailles, 26 février 2019, *Association des Juristes pour l'Enfance / OVH et Subrogalia SL*., n° 16/07633.
[365] TGI Brest, 11 juin 2013, *Josette B. / Catherine L., SAS-Overblog.*
[366] L'arrêt TGI Brest, 11 juin 2013, *Josette B. / Catherine L., SAS-Overblog,* en a déduit cette règle de la réserve d'interprétation posée par : Cons. const., 10 juin 2004, n° 2004-496 DC.
[367] Le caractère prompt du retrait fait l'objet d'une appréciation *in concreto* de la part du juge.V. par ex. : TGI Paris, 18 décembre 2007, *J.-Y. Lafesse et a. c/ Dailymotion*, n° 06/18289.
[368] PARLEMENT EUROPEEN, *Un régime de responsabilité civile pour l'intelligence artificielle* [en ligne], 20 octobre 2020, [consulté le 16 août 2021].

encore totalement réglées. La solution semble plutôt se diriger vers la possibilité d'un contrôle de ces algorithmes de recommandation par une autorité nationale, indépendamment du contrôle prévu pour les TGP au sein du DSA. Ce contrôle des règles constitutives de l'algorithme tenterait d'établir les circonstances d'un risque manifeste de préjudice collectif, s'entendant comme une atteinte au droit au contrôle du flux informationnel, mais aussi à la pluralité du contenu, mais aussi par une exposition abusive à la désinformation ou au contenu clivant du fait de règles algorithmiques favorisant ce type de contenu.

Cette responsabilité pourrait notamment s'inscrire à titre de seconde hypothèse, dans la mouvance d'une responsabilité conjointe, comme la CJUE a pu l'interpréter pour un administrateur de page fan, et Facebook concernant son action de paramétrage et de ciblage d'audience[369], mais qui serait partagée entre la plateforme et le fournisseur de l'algorithme de recommandation, s'il s'avère qu'ils sont des entités différentes.

Bien entendu, les connaissances actuelles des autorités sur ces algorithmes ne sont pas encore suffisantes afin de permettre à ces autorités de trancher sur les risques et comportements pouvant aboutir à cette forme de responsabilité. Il serait donc difficile de déterminer actuellement ce qui peut constituer un risque manifeste de préjudice collectif. Il sera donc nécessaire d'attendre les premiers résultats des contrôles et évaluations des risques prévus par les obligations imposées aux TGP. Cela permettra ainsi de disposer de connaissances et de données plus importantes sur la détermination de ces phénomènes. Pour reprendre ainsi les termes de Paula Forteza, ce n'est qu'en « *ouvrant la ''boite noire'' et en comprenant l'impact des réseaux sociaux sur nos sociétés que nous pourrons détailler des spécifications techniques* »[370].

Ces plateformes n'étant pas tributaires des lourdes obligations de transparence et de contrôle imposés aux TGP, la vérification des algorithmes de ces opérateurs passant entre les mailles du filet de la règlementation européenne pourrait se baser sur une enquête de ces autorités de contrôle nationales dès lors que des soupçons raisonnables d'atteinte au droit au contrôle du flux informationnel notamment serait établis. De ces contrôles pourrait aboutir l'attribution de sanctions proportionnées et dissuasives, à hauteur du chiffre d'affaires de l'entité gestionnaire de la plateforme. Il pourrait aussi en résulter une confiscation éventuelle de l'algorithme s'il

[369] CJUE, 29 juillet 2019, *Fashion ID GmbH & Co. KG*, aff. C-40/17.
[370] FORTEZA (P.), « Reprendre le contrôle des réseaux sociaux », *op. cit.* note 155.

était avéré qu'il ne sert finalement que pour une finalité illicite. La possibilité de recours auprès de juges nationaux tels que le Conseil d'État en France, puis au niveau européen la CJUE, participerait à la création d'une jurisprudence qui permettrait de délimiter avec plus de précision les contours du respect de ces nouveaux droits émergents, et par extension, des exigences en matière de responsabilité des plateformes. De l'interprétation de ce juge découleraient les principes de loyauté à respecter pour ces plateformes, ces avancées jurisprudentielles participant à la construction d'un véritable droit de la responsabilité algorithmique.

Il est à noter que dans ce cas de figure hypothétique, la logique d'autorégulation accompagnée d'un contrôle éventuel en cas de soupçons légitimes aurait toute sa place. La taille de ces plateformes étant plus basse que celle des TGP, mais plus nombreuses, les besoins matériels et humains pour assurer le respect effectif de ces règles serait trop importants. En empruntant à la logique de *privacy by design* et de *privacy by default* inhérents au RGPD, une déclinaison sous la forme de « *loyalty by design »* et de *« loyalty by default »* des règles algorithmiques sous-jacentes aux systèmes de recommandation serait pertinente.

C'est au demeurant ce que certains auteurs soutenaient à propos du contrôle effectif des obligations des plateformes, en évoquant la possibilité d'un développement de l'obligation de loyauté des plateformes. Cette obligation, déjà présente au sein de la loi pour une République numérique[371], pourrait être comprise comme une obligation transversale rééquilibrant les forces entre l'utilisateur et la plateforme[372]. Dans un objectif de réduire l'asymétrie informationnelle entre les plateformes d'un côté, et les régulateurs et utilisateurs de l'autre, de ce contrôle pourrait aboutir la vérification de nombreux principes déjà existants. Le principe de finalité notamment, dont l'analyse des règles algorithmiques pourrait permettre de constater si l'algorithme de recommandation agit bel et bien selon une « *finalité d'amélioration de l'expérience utilisateur d'un site* »[373], ou plutôt selon un objectif de captation déloyale de l'attention.

[371] Loi n° 2016-1321 du 7 octobre 2016 pour une République numérique, art. 49-52.
[372] SHULGA-MORSKAYA (T.), SANTOS (N.), « Les invisibilités » dans les campagnes électorales en ligne : quel encadrement juridique ? », p. 187, dans : NEVEJANS (N.), *Données et technologies numériques*, *op. cit.* note 168.
[373] HUBERT (G.), reprise des propos de ROUVROY (A.), « Algorithmes et responsabilités », *internetactu* [en ligne], 16 mars 2016, [consulté le 15 août 2021].

Enfin et pour conclure sur la responsabilisation des acteurs concernés par l'utilisation des systèmes de recommandation, la désignation d'une autorité pilote pouvant déployer ce type de contrôles pourrait directement être rattaché à l'une des autorités déjà existantes.

Cette option a notamment été évoquée dans un *rapport d'information sur les plateformes numériques*[374] déposé à l'Assemblée Nationale en juin 2020 par Valeria Faure-Mitian et Daniel Fasquelle. Ce rapport proposait notamment de créer une réglementation nationale *ex ante* au DSA, dans l'hypothèse où cette règlementation tarderait à entrer en application, tout en désignant l'Autorité de régulation des communications électroniques (ARCEP) en France, comme autorité compétente au contrôle des plateformes essentielles (ici les GAFAM et autres TGP)[375]. La réflexion de la présente recherche se positionne vers un contrôle plus étendu d'autres plateformes n'entrant pas dans cette qualification, que ce soit par l'ARCEP, ou par la création d'une autorité *ad hoc* disposant des outils de contrôle nécessaires, et qui s'intégrerait dans l'écosystème des autorités du numérique en ayant la mission de garantir l'application du droit de la régulation des plateformes.

Ces nouveaux apports juridiques plus spécifiques aux systèmes de recommandation ne pourraient suffire à assurer une véritable maitrise de ces outils, si les utilisateurs ne bénéficient guère de fonctionnalités suffisantes et d'une sensibilisation adéquate.

[374] FAURE-MITIAN (V.), FASQUELLE (D.), *Rapport d'information sur les plateformes numériques* [en ligne], Assemblée Nationale, 24 juin 2020, [consulté le 16 août 2021].
[375] *Ibid*., proposition n° 18.

## SECTION 2 – LA REPRISE EN MAIN DE LA SPHERE INFORMATIONNELLE PAR L'UTILISATEUR : UNE EXIGENCE FONDAMENTALE

Ces dernières années, de nombreuses actualités faisant mention de *bulle de filtre* ou de *chambre d'écho* ont été publiées sous des intitulés traduisant une réelle volonté de mettre fin à ces phénomènes. Dans une perspective de défense envers les utilisateurs, certains articles très évocateurs, invitent à « sortir de sa bulle de filtre »[376], voir même plus radicalement d' « éclater » cette bulle[377]. Pour limiter les effets de la désinformation lors de la pandémie, le rapport du CCDH proposait tout simplement à Instagram et son entité mère Facebook de retirer leurs algorithmes de recommandation, et de les réintroduire qu'à la condition d'y apporter des modifications les rendant sûrs[378]. Cette action aurait-elle pu limiter l'impact des campagnes de désinformation foisonnante en cette période ? Au vu des précédentes données, assurément.

Il ne faut pourtant pas se méprendre sur les caractéristiques de ce phénomène. Si la *bulle de filtre* peut apparaitre comme un effet néfaste des systèmes de recommandation, ces systèmes restent par nature des outils. Tout comme le chiffrement de bout-en-bout permet autant de protéger la vie privée des individus que de servir à des fins criminelles, les systèmes de recommandation peuvent contribuer à faciliter la vie des utilisateurs, ou au contraire participer à leur enfermement algorithmique.

C'est pourquoi il est apparu nécessaire de concilier les intérêts des individus et de la société, et l'usage fait par les plateformes de ces algorithmes de recommandation. Il a pu être constaté précédemment que cette conciliation pouvait principalement s'opérer par un encadrement juridique encore en formation en Europe.

Il est opportun de préciser que d'autres continents envisagent aussi une réponse juridique. Une proposition de loi Etatsunienne intitulée *Filter Bubble Transparency Act*[379] souhaitait en 2019 obliger les moteurs de recherche et réseaux sociaux à fournir une version non personnalisée des contenus recommandés par ces derniers. En somme, une disposition similaire à l'obligation de

[376] SCHMITT (C.), « Sortez de votre bulle ! », *France24* [en ligne], 19 octobre 2020, [consulté le 16 août 2021].
[377] KARAPINAR (O.), « Gabriel Weinberg : Faire éclater la bulle de filtrage », *Medium* [en ligne], 16 novembre 2020, [consulté le 16 août 2021].
[378] CENTER FOR COUNTERING DIGITAL HATE, *Malgorithm : how instagram's algorithm publishes misinformation and hate to millions during a pandemic, op. cit.* note 257, p. 37.
[379] S. 2763, 116th Congress, Filter Bubble Transparency Act [en ligne], 31 octobre 2019, [consulté le 16 août 2021].

proposer une option dénuée de profilage au sein de la proposition de législation sur les services numériques. Selon Eli Pariser, « *Le Filter Bubble Transparency Act permettrait de lever le voile sur ces algorithmes et aiderait les consommateurs à comprendre comment ils fonctionnent et à quel point les choix qu'ils font pour nous sont importants »*[380].

Cette conciliation peut s'opérer par les garanties juridiques précitées, mais aussi par l'attribution de nouvelles fonctionnalités pour les utilisateurs, ainsi que par une sensibilisation de ces derniers.

Cette dernière section s'émancipera davantage des dispositions juridiques, afin de proposer l'hypothèse d'une nouvelle classification du contenu en ligne (I), qui pourrait permettre à terme de faciliter la prise en main des systèmes de recommandation par les utilisateurs, mais aussi de contrer plus efficacement certains dangers émergents de l'incorporation de publicités de plus en plus subtiles au sein du contenu proposé dans la sphère numérique. Enfin, comme pour de nombreuses applications du numérique, la sensibilisation des utilisateurs constitue le jalon du processus de maitrise des systèmes de recommandation (II).

## I – L'hypothèse d'une nouvelle classification du contenu en ligne

Aux côtés de la transparence des algorithmes de recommandation, une réelle volonté de clarification du type de contenu informationnel ou publicitaire proposé se fait ressentir par différents acteurs.

Effectivement, le Conseil d'État constatait dans son avis politique de 2021 que les campagnes politiques utilisent de plus en plus les techniques de microciblage du secteur commercial ainsi que les techniques d'analyse du *Big data*[381]. De ce fait, ce dernier suggérait que les plateformes en ligne soient « *tenues de distinguer clairement les publicités à caractère politique des publicités à caractère commercial.* »[382].

[380] KAHN (S.), « Des sénateurs américains veulent faire éclater les bulles de filtre », *Le Figaro* [en ligne], 5 novembre 2019, [consulté le 16 août 2021].
[381] SENAT, *Avis politique sur la désinformation en ligne et les atteintes aux processus électoraux, op. cit.* note 142, cons. 54.
[382] *Ibid.*, cons. 100.

Sans surprise, la publicité politique a eu tendance à se confondre au sein de la publicité commerciale sur les réseaux sociaux. C'est un enseignement que Oana Goga, chercheuse au CNRS a pu présenter sous différents travaux. Interrogée par le Laboratoire d'Innovation Numérique de la CNIL (LINC)[383], Oana Goga affirmait que Facebook n'avait pas la compétence pour offrir une archive de publicités politiques dont on peut garantir sa complétude, et qu'aucune mesure permettant de détecter la publicité malveillante, par exemple en vérifiant le taux de clics, ou d'interactions sur la publicité (ce qui est sensiblement le même procédé permettant de détecter plus facilement la désinformation) n'avait été mise en place.

L'un de ses articles publiés sur le journal du CNRS, présentait le développement d'un outil nommé AdAnalyst, qui fonctionne à l'aide d'algorithmes de *machine learning*. Par l'utilisation de cet algorithme de classification, il a été montré qu'au moins la moitié des publicités politiques n'étaient pas répertoriées comme telles[384]. Par une analyse des publicités recommandées lors de la période des élections présidentielles au Brésil en 2018, environ 2% des publicités considérées comme commerciales étaient en réalité du contenu publicitaire politique, ce qui est un taux très important en réalité, compte tenu du taux de publicités politiques déclarés au sein du *Politcal Ad library* de Facebook estimé à environ 2% à 4%. Il s'agit là d'un réel problème démocratique, et plus encore lorsque des pays étrangers sont en capacité d'utiliser les mécanismes de la publicité afin d'influencer l'opinion publique des individus.

Force est de constater que sans obligation spécifique, les plateformes ne feront pas l'effort de permettre une véritable identification des publicités à visée politique, dont le même constat a été fait précédemment avec les pratiques de désinformation de manière plus générale. Les systèmes de recommandation, ayant été décriés pour leur rôle actif dans la propagation de ce contenu nuisible, ne pourraient-ils pas être revalorisés en véritable arme participant à lutter contre ce flou publicitaire ?

[383] VALLET (F.), « Oana Goga : « Facebook n'est pas compétent pour déterminer si une publicité est politique ou non » », *LINC* [en ligne], 28 janvier 2021, [consulté le 17 août 2021].
[384] GOGA (O.), « Les enjeux de la publicité politique ciblée », *Le journal CNRS* [en ligne], 17 juin 2021, [consulté le 17 août 2021].

En effet, le flux informationnel d'un utilisateur est géré par ces algorithmes, leur permettant de recevoir l'information pertinente pour eux, mais pourrait tout aussi bien disposer d'une nouvelle fonction de classification du type de contenu.

Cette tâche pourrait être mise en place à l'aide d'un algorithme de classification, de la même manière que l'équipe de recherche d'Oana Goga a réussi à identifier le type de contenu présent à l'aide du *machine learning*, avec un taux de faux positifs s'élevant uniquement à 1% (de publicités non politiques indiquées comme politique au sein de l'algorithme)[385]. Au sens de la présente recherche, les plateformes disposant des meilleures technologies en matière d'IA ne devraient pas avoir de difficultés à mettre en place un algorithme de *machine learning*, qui disposerait déjà du contenu nécessaire sur leurs propres plateformes en ligne afin de parvenir à un apprentissage automatique efficace de l'algorithme.

Il conviendrait par ailleurs d'étendre cette classification au-delà de la publicité. En effet, l'effacement de la publicité politique, et plus largement du contenu destiné à influencer les avis des utilisateurs, se dilue de plus en plus dans de nombreuses pratiques très discrètes. Pour la publicité simple, par exemple, il existe de nombreuses pratiques de publicité dissimulée qui s'intègrent dans un contenu informationnel standard. Cette pratique trompeuse considérée comme du *native advertising*, est censée être sanctionnée par le Code de la consommation[386], ainsi qu'empêchée par la LCEN exigeant que « *toute publicité, sous quelque forme que ce soit, accessible par un service de communication au public en ligne, doit pouvoir être clairement identifiée comme telle.* »[387]. Si ces protections s'appliquent très largement aux publicités commerciales dissimulées – comme peuvent en témoigner diverses sanctions à l'encontre de YouTubers par la Direction générale de la concurrence, de la consommation et de la répression des fraudes (DGCCRF)[388] – il est en définitive plus complexe d'identifier la nébuleuse de pratiques de manipulation politique et de publicités politiques s'intégrant dans de la publicité commerciale standard. Les difficultés vues précédemment des réglementations françaises et européennes à combattre ces pratiques ne contrediront pas cette affirmation.

[385] GOGA (O.), « Les enjeux de la publicité politique ciblée ». *op. cit.* note 384.
[386] C. consomm., art. L. 121-4.
[387] LCEN, art. 20.
[388] V. en ce sens : DGCCRF, « Paiement d'une amende de 20 000€ par l'influenceuse Nabilla BENATTIA-VERGARA, pour pratiques commerciales trompeuses sur les réseaux sociaux », [en ligne], 28 juillet 2021, [consulté le 17 août 2021].

C'est pourquoi la classification entre les publicités commerciales et politiques initialement faites, devrait être élargie en classification de contenu à vocation commerciale ou politique. Les applications concrètes de ces classifications permettraient par exemple aux utilisateurs, de gérer le niveau de recommandation d'un contenu en fonction de son identification. L'utilité principale de ce dispositif serait de diminuer l'impact du contenu politique (publicitaire ou non), voire néfaste au sens large, dès lors que ce dernier s'appuie sur des techniques de ciblage comportemental utilisées au sein du marketing. Effectivement, si l'identification de la manipulation politique par du contenu se dissimulant dans des catégories différentes de leur finalité initiale est compliquée, réduire l'exposition des individus visés par ces contenus serait un premier pas judicieux.

Cette classification pourrait à terme aller plus loin en permettant notamment de diversifier les paramétrages possibles avec une forte recommandation sur du contenu culturel, ou au contraire faible, afin de stimuler la découverte de nouvelles œuvres. Cette séparation pourrait même être adaptée avec une option permettant de favoriser la recommandation de contenus vérifiés par l'émergence des *fact-checker*. Le *fact-checking* (ou vérification des faits), est une pratique en plein développement, qui constitue un rempart supplémentaire contre les tentatives de manipulation de l'opinion publique. Cette position sur une fonctionnalité des algorithmes de recommandation permettant de privilégier le contenu vérifié a aussi été soutenue par Paula Forteza[389], députée ayant débattu notamment sur les lois du 22 décembre 2018.

En effet, certaines rubriques (dont certaines ne sont pas si récentes), tels que le « Factuel » de l'Agence France Presse (AFP), « Les décodeurs » du Monde, ou encore « Checknews » de Libération se sont données pour rôle de vérifier la véracité des informations en ligne[390]. Le développement d'outils de vérification des faits par les plateformes a aussi été encouragé par la recommandation du CSA de 2019 dans le cadre de la lutte contre la diffusion de fausses informations[391] et dès 2018 sur le plan européen avec le Code de bonnes pratiques en matière de lutte contre la désinformation[392].

[389] FORTEZA (P.), « Reprendre le contrôle des réseaux sociaux », *op. cit.* note 155.
[390] BERRICHE (M.), « Le Fact-checking est-il vraiment efficace ? », *SciencesPo* [en ligne], 22 janvier 2020, [consulté le 17 août 2021].
[391] CSA, 15 mai 2019, recommandation n° 2019-03, *op. cit.* note 230.
[392] COMMISSION EUROPEENNE, *EU code of Practice on Disinformation*, *op. cit.* note 245.

Le développement de ces initiatives, combiné à la possibilité pour les utilisateurs de configurer leurs systèmes de recommandation afin de privilégier ce type de contenu pourrait donc permettre de lutter plus efficacement contre la diffusion de ces fausses informations.

Naturellement, cette mise en pratique de fonctionnalités se basant sur une telle classification n'impacterai pas la propension dans laquelle le contenu à vocation politique, commerciale ou culturelle serait distribué au sein du flux informationnel des utilisateurs. Il en résulterait probablement une atteinte au droit à l'information, ainsi qu'à la diversité des opinions dans l'hypothèse où serait appliquée la recommandation de la Commission Nationale Consultative des Droits de l'Homme critiquée précédemment[393], consistant à ne plus proposer le contenu non désiré. Sans en modifier la proportion, il serait uniquement question de gérer la force de recommandation de l'algorithme par type de contenu.

Ensuite, cette classification n'aurait que pour seule vocation d'atteindre les règles algorithmiques de recommandation, et une fois encore, non le contenu en lui-même, puisqu'un risque de censure, qui plus est automatique, planerait sur tout type de contenu publié. Ce problème a été notamment mis en lumière par les algorithmes de modération de contenu de la plateforme YouTube, ayant bloqué la chaine d'un joueur d'échec pour avoir détecté les termes « noirs », « blancs » ou « attaque » dans la plupart des commentaires[394].

Certaines irrégularités de classification pourraient voir le jour, de la même manière que l'outil de l'étude d'Oana Goga a été déclaré comme présentant un taux de faux positifs de 1%. Si un tel niveau de classification exact était atteint, l'objectif de garantir le droit au contrôle du flux informationnel des individus sur les plateformes disposant de cet outil serait en grande partie atteint.

Enfin, il apparait nécessaire que les utilisateurs soient suffisamment sensibilisés afin de rendre ces nouvelles fonctionnalités effectives.

[393] CNDCH, *Avis relatif à la lutte contre la haine en ligne*, *op. cit.* note 342.
[394] « Une chaine YouTube d'échecs bloquée par une IA à cause des termes ''noirs'' et ''blancs'' », *Cnews* [en ligne], 2 février 2021, [consulté le 18 août 2021].

## II – La sensibilisation comme dernier jalon du processus de maitrise des systèmes de recommandation

Après l'algorithme, la plateforme, et la régulation, un dernier acteur entre en jeu. Il s'agit de l'utilisateur. La mise en place d'un arsenal juridique et technique serait peu utile sans la participation des utilisateurs à leur propre reprise de contrôle du flux informationnel auquel ils sont sujets. Dans la matrice du droit à l'autodétermination informationnelle, l'individu se trouve responsabilisé. Afin de pouvoir exercer ses droits, il est nécessaire qu'il devienne un acteur ayant la capacité de gérer les informations émises, mais aussi les informations reçues dans le cadre de recommandations algorithmiques.

Il peut être considéré que l'absence de compréhension claire par les individus du fonctionnement des plateformes qu'ils utilisent pour s'informer qui fait partie intégrante du problème. À ce titre, une étude a montré qu'en 2015, plus de 62% des utilisateurs de Facebook n'avaient encore aucune idée de l'activité éditoriale que joue l'algorithme, et croient que tous les *posts* de leurs amis et des pages qu'ils suivent apparaissent sur leur fil d'actualités[395].

Il s'agit là d'un taux relativement impactant, plus encore si l'on considère que la connaissance des procédés de recommandation permet aux individus de récupérer un certain contrôle sur leur flux informationnel. C'est ce qu'une autre étude de mai 2021 a pu avancer concernant les pratiques informationnelles des utilisateurs[396]. Plus l'usager est en capacité d'accumuler des éléments sur le fonctionnement du processus de filtrage du contenu, plus l'individu semble développer des comportements visant à reprendre un certain contrôle sur sa propre *bulle de filtre***.** L'étude en conclue que « *la composition d'un savoir technique fonctionnellement utile contribue à diminuer l'aliénation de l'usager* »[397].

Ce travail de sensibilisation a été réalisé en amont par de nombreuses initiatives. Il pourra être cité le travail de Guillaume Chaslot, l'ancien ingénieur ayant travaillé sur les systèmes de

[395] ESLAMI (M.), RICKMAN (A.), VACCARO (K.), « "I always assumed that I wasn't really that close to [her]": Reasoning about invisible algorithms in the news feed », *CHI '15: Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems* [en ligne], avril 2015, pp. 153-162, [consulté le 17 août 2017].
[396] CLAES (A.), WIARD (V.), MERCENIER (H.) et al., « Algorithmes de recommandation et culture technique : penser le dialogue entre éducation et design », *Tic et société* [en ligne], vol. 15 n° 1, pp. 127-157, [Consulté le 4 aout 2021].
[397] *Ibid*.

recommandation de la plateforme YouTube. Ce dernier a créé un site intitulé *Algotranparency*, ayant pour objectif que le grand public comprenne le fonctionnement des systèmes de recommandation et s'approprie au mieux cet outil[398]. Il pourra être cité de nombreuses applications qui permettent, en l'attente d'une véritable possibilité de naviguer sans être sujet aux recommandations, de naviguer sans être ciblé par le contenu recommandé. Le moteur de recherche DuckDuckGo propose quant à lui une navigation sans traceurs. D'autres initiatives venant plus simplement d'utilisateurs, proposent de sensibiliser les individus par le biais de vidéos de vulgarisation sur YouTube. Il pourra être notamment cité le Youtuber « Defakator », dont la finalité de la chaine est de sensibiliser le public aux fausses informations, au phénomène de *bulle de filtre* et aux autres procédés pernicieux proliférant au sein de l'univers numérique[399].

Il ne faudrait cependant pas se méprendre sur le rôle que devrait jouer l'État à ce sujet. Pour les utilisateurs en âge d'utiliser la technologie, de nombreuses formations au numérique sont dorénavant disponibles. La sensibilisation devrait d'autant plus être renforcée pour les plus jeunes générations. Déjà en 2015, un rapport de l'Agence nationale de la sécurité des systèmes d'information (ANSSI) plaçait les enjeux des nouvelles technologies au sein d'une stratégie nationale pour la sécurité du numérique, et considérait que « *la prise de conscience individuelle des risques liés à la numérisation de la société reste insuffisante* »[400].

Les enfants manquant de sensibilisation sont tout aussi impactés par les systèmes de recommandation. Au même titre que les données personnelles, le consentement des parents devrait être demandé préalablement à l'utilisation de ce type d'algorithme. Sans surprise, ce problème de sensibilisation n'est pas propre aux systèmes de recommandation, il est généralisé pour la plupart des enjeux du numérique.

Si une autorité devait être chargée de sensibiliser les individus aux impacts des algorithmes de recommandation, cette mission pourrait être accordée au CSA. En effet, cette autorité a déjà manifesté son intérêt pour ces algorithmes en menant différentes études ayant été mentionnées précédemment au sein de cette recherche[401]. Mais plus encore, le CSA s'est vu attribuer une

[398] V. en ce sens : Algotransparency.org, [en ligne], [consulté le 17 août 2021].
[399] Youtube, « Officiel DEFAKATOR », [en ligne], [consulté le 17 août 2021].
[400] ANSSI, *Stratégie nationale pour la sécurité du numérique* [en ligne], 16 octobre 2015, [consulté le 17 août 2021].
[401] CSA, *Capacité à informer des algorithmes de recommandation : Une expérience sur le service Youtube*, *op. cit.*, note 4.

mission de protection de la jeunesse très tôt, puisque dès sa création en 1989, ce dernier a établi la signalétique jeunesse[402], destinée à protéger les plus jeunes de programmes non adaptés. Plus récemment, le CSA se trouve être en processus de fusion avec la Haute autorité pour la diffusion des œuvres et la protection des droits sur Internet (HADOPI), afin de créer l'Autorité de régulation de la communication audiovisuelle et numérique (ARCOM)[403]. Bien que le CSA ne souhaite pas être le gendarme de l'internet, il s'agit là de l'autorité toute désignée pour superviser la sensibilisation des utilisateurs aux systèmes de recommandation.

L'action des autorités n'est pourtant pas la plus visible. Paradoxalement, ce sont les personnalités ayant le plus à attendre des systèmes de recommandation, tel que les YouTubers, ou de manière générale, les influenceurs, qui sont aujourd'hui les mieux à même de transmettre le message.

Si le RGPD est le Cheval de Troie de la conformité dans le monde, le créateur de contenu s'avère être le Cheval de Troie de l'obscurantisme teintant les systèmes de recommandation.

[402] V. en ce sens : CSA, « La signalétique jeunesse », [en ligne], [consulté le 17 août 2021].
[403] AFP, « Le Sénat approuve la fusion entre le CSA et l'HADOPI », *Stratégie* [en ligne], 21 mai 2021, [consulté le 18 août 2021].

## CONCLUSION DE LA SECONDE PARTIE

La mise en place à venir du DSA induit de nouveaux espoirs quant à la prise en main de l'UE des systèmes de recommandation utilisés par les TGP. Les nouvelles obligations de contrôle et de transparence doivent permettre de réduire les risques de ces algorithmes, et leur utilisation à des fins préjudiciables pour la société. Que ce soit du point de vue de ces obligations, mais aussi des fonctionnalités à faire émerger, plusieurs acteurs se sont positionnés pour un renforcement de cet encadrement.

Toute la problématique actuelle est alors la question de l'effectivité de ces mesures, et de la manière dont la Commission européenne notamment, arrivera à affirmer sa volonté de faire respecter le droit européen et ses grands principes.

Les potentielles lacunes de cette proposition quant à son champ d'application, amène à considérer qu'il est nécessaire de développer un droit transversal au contrôle du flux informationnel. En effet, des obligations lourdes et contraignantes sont à venir pour les TGP, mais les processus préjudiciables issus de l'économie de l'attention doivent être combattus à toutes les échelles, avec des obligations moins contraignantes et plus flexibles pour les plateformes à taille réduite.

Ainsi, les autorités nationales doivent être en mesure de contrôler les règles algorithmiques susceptibles de recommander plus facilement du contenu clivant ou de la désinformation, et plus encore lorsqu'il est admis que certaines ingérences d'États étrangers puissent se manifester sur des territoires et plateformes plus circonscrites. Cela aboutira finalement à de probables recours juridictionnels permettant de délimiter les contours du respect de ces droits émergents, et de fournir une interprétation qui pourra constituer une prémisse supplémentaire au droit de la responsabilité algorithmique.

Les concepts de *privacy by design* ou de *privacy by default* inhérents au RGPD gagneraient à s'étendre au-delà des exigences de la protection des données, et de se décliner sous une variante de « *loyalty by design* » et de « *loyalty by default* » des règles algorithmiques chargés de l'organisation du flux informationnel auquel les individus sont sujets au quotidien. Ce contrôle des risques des systèmes de recommandation serait naturellement circonscrit au contrôle de

règles algorithmiques privilégiant le contenu nuisible, et ne concernerait ni le contrôle du contenu en lui-même – des dispositions portant sur la qualification du contenu manifestement illicite accomplissent déjà cette tâche – ni sur l'utilisateur, afin de garantir la protection de la liberté d'expression et prévenir les risques de censure (risques ayant déjà été exposés lors de la censure quasi-intégrale de la loi Avia).

Enfin ces nouveaux outils juridiques ne sauraient s'appliquer en l'absence de fonctionnalités supplémentaires permettant un contrôle effectif du flux informationnel pour l'individu, qui doit impérativement être sensibilisé à ces enjeux. Dès lors, un travail d'information à plusieurs niveaux doit être effectué pour les utilisateurs actuels, mais aussi plus les générations à venir.

# CONCLUSION GENERALE

Le présent mémoire a eu pour ambition principale de rendre compte de l'impact que pouvait avoir les systèmes de recommandation. Il est à ce sujet, parfois défendu l'idée d'un éclatement de la *bulle de filtre*, ou de s'en dépêtrer. Cette volonté est pourtant contre-productive. Bien que la présente recherche se soit évertuée à dénoncer certains de ses dangers, la *bulle de filtre* n'est rien d'autre qu'une métaphore traduisant les effets d'outils algorithmiques de recommandation, qui s'avèrent désormais indispensables au contrôle du flux informationnel. Sûrement par un « effet cliquet » technologique, il n'est pas envisageable (ni souhaitable dans ce cas précis) de renoncer à ces algorithmes. Leur maitrise, leur compréhension, ainsi que leur encadrement – juridique et technique – s'avère être un enjeu dont l'importance a été progressivement comprise par les régulateurs, activistes, chercheurs, et utilisateurs.

L'encadrement lacunaire dont ces systèmes ont fait l'objet était principalement induit par une asymétrie informationnelle encore trop prononcée, entre l'utilisation de ces algorithmes par les grandes plateformes, et leur appréhension par les acteurs extérieurs. Le *Digital Service Act* constitue la première véritable clé, qui permettra indéniablement de nourrir les recherches à venir et d'ouvrir un peu plus aux yeux du monde la « boite noire » de ces algorithmes. Cette réglementation n'est cependant qu'un début, et offre un cadre légal encore partiel pour assurer la lutte contre la désinformation, ainsi que le respect de la liberté d'opinion, et d'information en Europe[404].

Si la thèse de ce mémoire devait être résumée en une phrase, celle-ci consisterait à souligner que les droits et libertés des individus ont été éprouvés par l'utilisation de systèmes à l'encadrement lacunaire, pour être ensuite mieux considérés par les projets de règlementation à venir, projets qui devront bénéficier de garanties transversales et multidisciplinaires.

À l'image de l'allégorie de la caverne de Platon[405], si la technologie doit jouer un rôle dans la perception que l'humain aura de son environnement, cette dernière ne doit non pas l'influencer et maintenir son attention sur des projections déformées, mais plutôt lui permettre de se retourner et d'approcher, du mieux qu'il le pourra, la Vérité.

[404] POULLET (Y.), RUFFO DE CALABRE (M.-N.), « La régulation des réseaux sociaux », *op. cit.* note 90.
[405] PLATON, *La République Livre VII*, *op. cit.* note 1.

# BIBLIOGRAPHIE

## I. OUVRAGES GENERAUX ET SPECIALISES


**- A -**

**AFP**, « Le Sénat approuve la fusion entre le CSA et l'HADOPI », *Stratégie*, 21 mai 2021, disponible en ligne : https://www.strategies.fr/actualites/medias/4061810W/le-senat-approuve-la-fusion-entre-le-csa-et-l-hadopi.html [consulté le 18 août 2021].

**ARCELIN (L.), FOURGOUX (J.-L.)**, *Droit du marché numérique*, LGDJ, vol. 18, Coll. Les Intégrales, 1ère éd., 2021, 408 p., IBSN : 978-2-275-07176-3.

**- B -**

**BASDEVANT (A.), MIGNARD (J.-P.)**, *L'empire des données*, Don Quichotte, 2018, 360 p., ISBN : 978-2-359-49635-2.

**BENSAMOUN (A.) (dir.), LOISEAU (G.) (dir.)**, *Droit de l'intelligence artificielle*, LGDJ, vol. 15, Coll. Les Intégrales, 1ère éd., 2019, 444 p., ISBN : 978-2-275-06564-9.

**BRONNER (G.)**, *La démocratie des crédules*, Ed. PUF, 2013, 360 p., ISBN : 978-2-13-060729-8.

**- C -**

**CARDON (D.)**, *À quoi rêvent les algorithmes*, Ed. Seuil, 2015, 112 p., ISBN : 978-2-021-27996-2.

**CHAUVIERE (F.)**, *Les grandes épopées qui ont fait la science*, Ed. Flammarion, Coll. Champs-Sciences, 2020, 288 p., ISBN : 978-2-081-43359-5

**- D -**

**D'ASCOLI (S.)**, *Comprendre la révolution de l'intelligence artificielle*, Ed. First, 2020, 192 p., ISBN : 978-2-412-05591-5.

**DESMOULIN-CANSELIER (S.), LE METAYER (D.)**, *Décider avec les algorithmes, quelle place pour l'homme, quelle place pour le droit* ?, Ed. Dalloz, 2020, 275 p., ISBN : 978-2-247-19539-8.

**DURIEUX (E.)**, *Droit des médias*, LGDJ, 8e ed., 2018, 996 p., ISBN : 978-2-275-03873-5.

**- F -**

**FERAL-SCHUHL (C.)**, *Cyberdroit*, 2020/2021, Ed. Dalloz, 2020, 1194 p., ISBN : 978-2-247-19581-7.

**- K -**

**KEYES (**R.), *The Post-truth Era: Dishonesty And Deception In Contemporary Life*, Ed. First, 2004, 312 p., ISBN : 978-0-312-30648-9

**KOENIG (G.)**, *La fin de l'individu : voyage d'un philosophe au pays de l'intelligence artificielle*, ed. L'observatoire, 2019, 400 p., ISBN : 979-1-032-90720-7.

**- L -**

**LESSIG (L.)**, *Code : And Other Laws of Cyberspace, Version 2.0*, Basic Books, 2006, 242 p., ISBN : 978-0-465-03914-2.

**LUC (J.)**, *L'intelligence artificielle n'existe pas*, ed. First, 2019, 200 p., ISBN : 978-2-412-04340-0.

**- M -**

**MENECEUR (Y.)**, *L'intelligence artificielle en procès : Plaidoyer pour une réglementation internationale et européenne*, Ed. Bruylant, 2020, 450 p., ISBN : 978-2-8027-6588-2.

**- N -**

**NEVEJANS (N.)**, *Données et technologies numériques*, ed. Mare & Martin, Coll. Droit & Science politique, 2021, 350 p., ISBN : 978-2-84934-561-0.

**- P -**

**PARISER (E.)**, *The filter bubble: What The Internet Is Hiding From You*, ed. Penguin Group, 2011, 304 p., ISBN : 978-0241954522.

**POULLET (Y.)** (dir.), *Vie privée, liberté d'expression et démocratie dans la société numérique*, ed. Larcier, 2020, 258 p., ISBN : 978-2-8079-2124-5.

**- S -**

**SUMPTER (D.)**, *Outnumbered : From Facebook and Google to fake news and filter-bubbles – the algorithms that control our lives*, Blommsbury Publishing, 2018, 288 p., ISBN : 978-1-4729-4742-0.

**- T -**

**THALER (R.), SUNSTEIN (C.)**, *Nudge: Improving Decisions About Health, Wealth, and Happiness*, Yale University Press, 2008, 304 p., ISBN : 978-0-300-12223-7.

**- Z -**

**ZUBOFF (S.)**, *L'âge du capitalisme de surveillance*, Zulma, 2020, 856 p., ISBN : 978-2-84304-926-2.

## II. THESES, ESSAIS

**- G -**

**GROSSETTI (Q.)**, « Système de recommandation sur les plateformes de micro-blogging et bulles filtrantes », *Réseaux sociaux et d'information*, thèse, Sorbonne Université, 2018, disponible en ligne : https://tel.archives-ouvertes.fr/tel-02868050/document [consulté le 5 août 2021].

## III. DICTIONNAIRES, LEXIQUES, REPERTOIRES, ENCYCLOPEDIES

**- J -**

**JOURNAL OFFICIEL DE LA REPUBLIQUE FRANÇAISE**, *Vocabulaire de l'intelligence artificielle (liste de termes, expressions et définitions adoptées)*, JORF n° 0285, texte n°58, 9 décembre 2018, disponible en ligne : https://www.legifrance.gouv.fr/jorf/article_jo/JORFARTI000037783814 [consulté le 27 juillet 2021].

**- L -**

**LAROUSSE,** *Encyclopédie Larousse en ligne*, Intelligence artificielle, disponible en ligne : https://www.larousse.fr/encyclopedie/divers/intelligence_artificielle/187257 [consulté le 28 juillet 2021].

**- O -**

**OFFICE QUEBECOIS DE LA LANGUE FRANÇAISE**, *Grand dictionnaire terminologique*, disponible en ligne : http://www.oqlf.gouv.qc.ca/accueil.aspx [consulté le 5 août 2021].

**OXFORD LEARNER'S DICTIONARIES,** *Dictionnaire d'Oxford*, disponible en ligne : https://www.oxfordlearnersdictionaries.com/ [consulté le 6 août 2021].

**- W -**

**WIKIPEDIA**, disponible en ligne : https://fr.wikipedia.org/wiki/Wikip%C3%A9dia:Accueil_principal [consulté le 8 août 2021].

## IV. ARTICLES DE REVUE, CONTRIBUTIONS

**- A -**

**ABADI (M.), ANDERSEN (D. G.)**, « Learning to Protect Communications with Adversarial Neural Cryptography », *ArXiv*, 24 octobre 2016, disponible en ligne : https://arxiv.org/abs/1610.06918 [consulté le 26 juillet 2021].

**- B -**

**BACCOU (R.)**, « Le récit de l'allégorie de la Caverne », *Horizons philosophiques*, Vol. 9 n°2, pp. 21–25, traduction de : **PLATON**, *La République Livre VII*, Garnier-Flammarion, Paris, 1987, pp. 273-276, disponible en ligne : https://www.erudit.org/fr/revues/hphi/1999-v9-n2-hphi3190/801123ar/ [consulté le 28 juillet 2021].

**BAKSHY (E.), MESSING (S.), ADAMIC (L.)**, « Exposure to ideologically diverse news and opinion on Facebook », *Sciences*, vol. 348, issue 6239, 5 juin 2015, pp. 1130-1132, disponible en ligne : https://science.sciencemag.org/content/348/6239/1130.full [consulté le 1 août 2021]. DOI : 10.1126/science.aaa1160.

**BARBERA (P.), JOST (J.T.), NAGLER (J.) et al.**, « Tweeting From Left to Right : Is online Political Communication More Than an Echo Chamber? », *Psychological Science*, vol. 26 n°10 (2015) : 1531-42, Octobre 2015, disponible en ligne :

https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.715.7520&rep=rep1&type=pdf [consulté le 28 juillet 2021]. DOI : 10.1177/0956797615594620.

**BODO (B.), HELBERGER (N.), VREESE (C. H.)**, « Political micro-targeting », *Internet Policy Review*, vol. 6 n° 4, 20 décembre 2017, disponible en ligne : https://policyreview.info/articles/analysis/political-micro-targeting-manchurian-candidate-or-just-dark-horse [consulté le 3 août 2021]. DOI : 10.14763/2017.4.776.

**BOURREAU (M.), PERROT (A.)**, « Plateformes numériques : réguler avant qu'il ne soit trop tard », *Notes du conseil d'analyse économique*, vol. 60 n°6, 2020, pp. 1-12. Disponible en ligne : https://www.cairn.info/revue-notes-du-conseil-d-analyse-economique-2020-6-page-1.htm [consulté le 4 aout 2021]. DOI : 10.3917/ncae.060.0001.

**BRUNESSEN (B.)**, « Chronique Droit européen du numérique – La volonté de réguler les activités numériques », *RTD Eur.*, 2021, p. 160.

**- C -**

**CARAMOZZINO (E.)**, « Le profilage encadré pour favoriser la diversité culturelle », *Dalloz JAC 2016*, n° 36, p. 6.

**CASTAGNOS (S.), BRUN (A.), BOYER (A.)**, « La diversité : entre besoin et méfiance dans les systèmes de recommandation » *Revue I3 - Information Interaction Intelligence*, Cépaduès, 2014, p. 3, disponible en ligne : https://hal.inria.fr/hal-01108998/document [consulté le 24 juillet 2021].

**CITTON (Y.)**, « Introduction », dans : **CITTON (Y.)**, *L'économie de l'attention. Nouvel horizon du capitalisme ?* La Découverte, 2014, pp. 7-31, disponible en ligne : https://www.cairn.info/l-economie-de-l-attention--9782707178701-page-7.htm [consulté le 5 août 2021].

**CLAES (A.), WIARD (V.), MERCENIER (H.) et al.**, « Algorithmes de recommandation et culture technique : penser le dialogue entre éducation et design », *Tic et société*, vol. 15 n° 1, pp. 127-157, disponible en ligne : https://journals.openedition.org/ticetsociete/5915 [consulté le 4 août 2021]. DOI : 10.4000/ticetsociete.5915.

**CLAUDEL (E.)**, « Numérique : le droit de la concurrence français à l'offensive », *RTD Com.*, 2020, p. 806.

**COPAIN-HERITIER (C.)**, « Le cadre européen de la protection des données : entre forces et faiblesses intrinsèques », *Rev. UE*, 2021, p. 163.

**CREEMERS (R.)**. « Comment la Chine projette de devenir une cyber-puissance », *Hérodote*, vol. 177-178, n° 2-3, 2020, pp. 297-311, disponible en ligne : https://www.cairn.info/revue-herodote-2020-2-page-297.htm?ref=doi [consulté le 15 août 2021].

**- D -**

**DE MARCELLIS-WARIN (N.), MARTY (F.), THELISSON (E.)** et al., « Intelligence artificielle et manipulations des comportements de marché : l'évaluation ex ante dans l'arsenal du régulateur », *RIDE*, Vol. XXXIV n° 2, 2020, pp. 203-245, disponible en ligne : https://www.cairn.info/revue-internationale-de-droit-economique-2020-2-page-203.html [consulté le 4 août 2021]. DOI : 10.3917/ride.342.0203.

**DOBBER (T.), TRILLING (D.), HELBERGER (N.)** et al., « Two crates of beer and 40 pizzas: the adoption of innovative political behavioural targeting techniques », *Internet Policy Review*, vol. 6 n° 4, 18 octobre 2017, disponible en ligne : https://policyreview.info/articles/analysis/two-crates-beer-and-40-pizzas-adoption-innovative-political-behavioural-targeting [consulté le 3 août 2021]. DOI : 10.14763/2017.4.777.

**DOMMETT (K.), POWER (S.)**, « The Political Economy of Facebook Advertising: Election Spending, Regulation and Targeting Online », *The Political Quarterly*, vol. 90 n° 2, avril 2019, disponible en ligne : https://www.researchgate.net/publication/332783668_The_Political_Economy_of_Facebook_Advertising_Election_Spending_Regulation_and_Targeting_Online [consulté le 4 août 2021].

**- G -**

**GEROT (M.), MAXWELL (W.)**, « Le RGPD pourrait freiner les ambitions de l'Europe en matière d'intelligence artificielle », *Gaz. Pal.*, 23 juin 2020, n° 381k0, p. 16.

**GESCHKE (D.), LORENZ (J.), HOLTZ (P.)**, « The triple-filter bubble: Using agent-based modelling to test a meta-theoretical framework for the emergence of filter bubbles and echo chambers », *British Journal of Social Psychology*, vol. 58 n° 1, pp. 129-149, disponible en ligne : https://pubmed.ncbi.nlm.nih.gov/30311947/ [consulté le 1 août 2021]. DOI : 10.1111/bjso.12286.

**GOLA (R.)** « Publicité digitale et encadrement des algorithmes », *RLDI*, n° 141, 1 octobre 2017.

**- H -**

**HARDCASTLE (S.), HAGGER (M.)**, « Psychographic Profiling for Effective Health Behavior Change Interventions », *Health Psychologu and Behavioural Medicine Research Group*, Université de Curtin, 6 janvier 2016, disponible en ligne : https://www.frontiersin.org/articles/10.3389/fpsyg.2015.01988/full [consulté le 27 juillet 2021]. DOI : 10.3389/fpsyg.2015.01988.

**HERBERT (S.)**, « Designing Organizations for an Information-Rich World », dans : **GREENBERGER (M.)**, *Computers, communications, and the public interest*, The John Hopkins Press, 1971, pp. 38-72, disponible en ligne : https://cosimoaccoto.com/2013/03/09/designing-organizations-for-an-information-rich-world-1969/ [consulté le 5 août 2021].

**HORTA RIBEIRO (M.), OTTONI (R.), WEST (R.)**, et al., « Auditing Radicalization Pathways on YouTube », *Computers and Society*, 22 août 2019, disponible en ligne : https://arxiv.org/abs/1908.08313 [consulté le 2 août 2021].

**- J -**

**JIANG (R.), CHIAPPA (S.), LATTIMORE (T.)** et al., « Degenerate Feedback Loops in Recommender Systems », *Proceedings of AAAI/ACM Conference on AI, Ethics, and Society*, janvier 2019, disponible en ligne : https://arxiv.org/abs/1902.10730 [consulté le 4 août 2021].

**- K -**

**KALT (B.)**, « The Perfect Crime », *Georgetown Law Journal*, vol. 93, 2005, pp. 675-688, disponible en ligne : https://papers.ssrn.com/sol3/cf_dev/AbsByAuth.cfm?per_id=327573 [consulté le 1 août 2021].

**KALTHEUNER (F.), BIETTI (E.)**, « Data is power: Towards additional guidance on profiling and automated decision-making in the GDPR », *Journal of Information Rights Policy and Practice*, vol. 2 n° 2, Janvier 2018, disponible en ligne : https://www.researchgate.net/publication/322620145_Data_is_power_Towards_additional_guidance_on_profiling_and_automated_decision-making_in_the_GDPR [consulté le 3 août 2021]. DOI : 10.21039/irpandp.v2i2.45.

**- L -**

**LARRERE (C.)**, « Le principe de précaution et ses critiques », *Innovations*, vol. n° 18, n° 2, 2003, pp. 9-26, disponible en ligne : https://www.cairn.info/revue-innovations-2003-2-page-9.htm [consulté le 29 juillet 2021].

**- M -**

**MARTY (F.)**, « La protection des algorithmes par le secret des affaires. Entre risques de faux négatifs et risques de faux positifs », *RIDE*, 2019/2 (t. XXXIII), pp. 211-237, disponible en ligne : https://www.cairn.info/revue-internationale-de-droit-economique-2019-2-page-211.htm [consulté le 15 août 2021].

**MARTY (F.)**, « Pratiques anticoncurrentielles algorithmiques : une revue de littérature », *Groupe de recherche en Droit, Économie et Gestion (Gredeg)*, Université Côte d'azur, 2021, disponible en ligne : http://www.gredeg.cnrs.fr/working-papers/GREDEG-WP-2021-21.pdf [consulté le 4 août 2021].

**MAYER-SCHÖNBERGER (V.), PADOVA (Y.)**, « Regime Change? Enabling Big Data through Europe's New Data Protection Regulation », Science and Technology Law Review, vol. 17 n° 2, 2016, pp. 315-335, disponible en ligne : https://doi.org/10.7916/stlr.v17i2.4007 [consulté le 29 juillet 2021].

**MENDOZA-CAMINADE (A.)**, « Big data et données de santé : quelles régulations juridiques ? », *RLDI*, n° 127, 1er juin 2016.

**- P -**

**POIRIER (D.), FESSANT (F.), TELLIER (I.)**, « De la Classification d'Opinion à la Recommandation : l'Apport des Textes Communautaires », *Revue TAL*, Opinions, sentiments et jugements d'évaluation, vol. 51 n° 3, 2010, p. 22, disponible en ligne : https://hal.inria.fr/inria-00597394/document [consulté le 29 juillet 2021]. HAL Id : inria-00597394.

**POULLET (Y.), RUFFO DE CALABRE (M.-N.)**, « La régulation des réseaux sociaux », *Études*, vol. 6, 2021, pp. 19-30, disponible en ligne : https://www.cairn.info/revue-etudes-2021-6-page-19.htm [consulté le 1 août 2021].

**PRIETO (C.)**, « Nouveaux abus de position dominante de Google : après celui lié à Google Shopping, ceux relatifs à Android », *RTD eur.*, 2018, p. 513.

**- R -**

**RAMBAUD (R.)**, « lutter contre la manipulation de l'information », *AJDA 2019*, p. 453.

**ROCHFELD (J.)**, « L'encadrement des décisions prises par algorithme », Dalloz IP/IT 2018, pp. 474.

**ROUAULT (M.)**, « Chapitre IX. Décision et apprentissage », dans : **COLLINS (T.)**, *La cognition. Du neurone à la société*, Gallimard, Folio Essais, 2018, pp. 371-419, disponible en ligne : https://www-cairn-info.ressources-electroniques.univ-lille.fr/la-cognition--9782072764370-page-371.htm [consulté le 1 août 2021].

**ROUVROY (A.), BERNS (T.)**, « Gouvernementalité algorithmique et perspectives d'émancipation », *Réseaux*, vol. 177, n° 1, 2013, pp. 163-196, disponible en ligne : https://www.cairn.info/revue-reseaux-2013-1-page-163.htm [consulté le 26 juillet 2021].

**- S -**

**SERUGA-CAU (E.), HAVEL (T.)**, « Campagne électorale et utilisation des données personnelles : grands principes et points de vigilance », *AJCT*, février 2019, pp. 73-75, disponible en ligne : https://www.cnil.fr/sites/default/files/atoms/files/campagne-electorale-donnees-personnelles.pdf [consulté le 4 août 2021].

**SHULGA-MORSKAYA (T.), SANTOS (N.)**, « Les invisibilités » dans les campagnes électorales en ligne : quel encadrement juridique ? », pp. 177-187, dans : **NEVEJANS (N.)**, *Données et technologies numériques*, ed. Mare & Martin, coll. Droit et Science politique, 2021, 350 p.

**- T -**

**TURING (A. M.)**, « Computing Machinery and Intelligence », *Mind*, New Series, Vol. 59, No. 236, 1950, pp. 433-460, disponible en ligne : https://www.csee.umbc.edu/courses/471/papers/turing.pdf [consulté le 26 juillet 2021].

**TÜRK (P.)**, « L'autodétermination informationnelle : un droit fondamental émergent ? », *Dalloz IP/IT*, 2020, p. 616.

**- V -**

**VILLANI (C.)**, « La mathématique n'est pas qu'une matière abstraite », in CHAUVIERE (F.), *Les grandes épopées qui ont fait la science*, Ed. Flammarion, 2020, pp. 255-281.

**- Z -**

**ZARATE (P.)**, « L'intelligence artificielle d'hier à aujourd'hui », *Dalloz Droit Social*, 2 février 2021, pp. 106-109.

## V. ARTICLES DE PRESSE

« Des utilisateurs de Facebook « manipulés » pour une expérience psychologique », *Le monde*, 30 juin 2014, disponible en ligne : https://www.lemonde.fr/pixels/article/2014/06/30/des-utilisateurs-de-facebook-manipules-pour-une-experience-psychologique_4447625_4408996.html [consulté le 1 août 2021].

« Une chaine YouTube d'échecs bloquée par une IA à cause des termes ''noirs'' et ''blancs'' », *Cnews*, 2 février 2021, disponible en ligne : https://www.cnews.fr/monde/2021-02-23/une-chaine-youtube-dechecs-bloquee-par-une-ia-cause-des-termes-noirs-et-blancs [consulté le 18 août 2021].

**- B -**

**BARTHELEMY (P.)**, « Comment les grandes marques influent sur nos cerveaux », *Le monde*, 16 juin 2013, disponible en ligne : https://www.lemonde.fr/passeurdesciences/article/2013/06/16/comment-les-grandes-marques-influent-sur-nos-cerveaux_5998913_5470970.html [consulté le 15 août 2021].

**BARTHELEMY (P.)**, « Garry Kasparov – Deep Blue : échec et bug », *Le monde*, 21 juillet 2015, disponible en ligne : https://www.lemonde.fr/festival/article/2015/08/22/garry-kasparov-deep-blue-echec-et-bug_4733491_4415198.html [consulté le 26 juillet 2021].

**BERRICHE (M.)**, « Le Fact-checking est-il vraiment efficace ? », *SciencesPo*, 22 janvier 2020, disponible en ligne : https://www.sciencespo.fr/actualites/actualit%C3%A9s/le-fact-checking-est-il-vraiment-efficace/4539 [consulté le 17 août 2021].

**- C -**

**CNIL**, « L'autorité luxembourgeoise de protection des données a prononcé à l'encontre d'Amazon Europe Core une amende de 746 millions d'euros », 3 août 2021, disponible en ligne : https://www.cnil.fr/fr/lautorite-luxembourgeoise-de-protection-des-donnees-prononce-lencontre-damazon-europe-core-une [consulté le 5 août 2021].

**CNIL**, « Cookies et autres traceurs : la CNIL publie des lignes directrices modificatives et sa recommandation », 1 octobre 2020, disponible en ligne : https://www.cnil.fr/fr/cookies-et-autres-traceurs-la-cnil-publie-des-lignes-directrices-modificatives-et-sa-recommandation, [consulté le 3 août 2021].

**COMMISSION EUROPEENNE**, « Final results of the Eurobarometer on fake news and online disinformation », *Shaping Europe's digital future*, 12 mars 2018, disponible en ligne : https://digital-strategy.ec.europa.eu/en/final-results-eurobarometer-fake-news-and-online-disinformation [consulté le 11 août 2021].

**CRICHTON (C.)**, « Le Digital Service Act, un cadre européen pour la fourniture de services en ligne », *Dalloz actualité*, 8 janvier 2021, disponible en ligne : https://www.dalloz-actualite.fr/flash/digital-service-act-un-cadre-europeen-pour-fourniture-de-services-en-ligne [consulté le 9 août 2021].

**CRICHTON (C.),** « Projet de règlement sur l'IA (II) : une approche fondée sur les risques », *Dalloz actualité*, 4 mai 2021, disponible en ligne : https://www.dalloz-actualite.fr/flash/projet-de-reglement-sur-l-ia-ii-une-approche-fondee-sur-risques [consulté le 13 août 2021].

**CSA**, « La signalétique jeunesse », disponible en ligne : https://www.csa.fr/Proteger/Protection-de-la-jeunesse-et-des-mineurs/La-signaletique-jeunesse [consulté le 17 août 2021].

**CSA**, « Le CSA expose sa vision d'une nouvelle régulation européenne », *11e réunion de l'ERGA*, 27 juin 2019, disponible en ligne : https://www.csa.fr/Reguler/Regulation-europeenne-et-internationale/Le-CSA-et-l-Union-Europeenne-l-ERGA/Le-CSA-expose-sa-vision-d-une-nouvelle-regulation-europeenne [consulté le 7 août 2021].

**- D -**

**DE (F.)**, « On vous a menti ! Souffler dans les cartouches ne sert à rien ! », *Hitek*, 3 juillet 2014, disponible en ligne : https://hitek.fr/actualite/tort-souffler-cartouche-nes_3169 [consulté le 6 août 2021].

**DGCCRF**, « Paiement d'une amende de 20 000€ par l'influenceuse Nabilla BENATTIA-VERGARA, pour pratiques commerciales trompeuses sur les réseaux sociaux », 28 juillet 2021, disponible en ligne : https://www.economie.gouv.fr/dgccrf/paiement-dune-amende-de-20-000eu-par-linfluenceuse-nabilla-benattia-vergara-pour-pratiques [consulté le 17 août 2021].

**- F -**

**FORTEZA (P.)**, « Reprendre le contrôle des réseaux sociaux », *Fondation Jean Jaurès*, 8 décembre 2020, disponible en ligne : https://www.jean-jaures.org/publication/reprendre-le-controle-des-reseaux-sociaux/ [consulté le 5 août 2021].

**- G -**

**G'SELL (F.)**, « qu'est-ce que la souveraineté numérique ? », *Chaire Digital, Gouvernance et Souveraineté*, 9 juillet 2020, disponible en ligne : https://www.sciencespo.fr/public/chaire-numerique/2020/07/09/quest-ce-que-la-souverainete-numerique/ [consulté le 8 août 2021].

**GATELAIS (S.)**, « "Post-vérité", élu mot de 2016 : de Trump au Brexit, le reflet d'une année populiste », *Le Nouvel* Obs, 21 novembre 2016, disponible en ligne : https://leplus.nouvelobs.com/contribution/1600188-post-verite-elu-mot-de-2016-de-trump-au-brexit-le-reflet-d-une-annee-populiste.html [consulté le 6 août 2021].

**GEORGES (B.)**, « Le talon d'Achille de l'intelligence artificielle », *Les échos*, 15 mai 2017, disponible en ligne : https://www.lesechos.fr/2017/05/le-talon-dachille-de-lintelligence-artificielle-168099 [consulté le 5 août 2021].

**GOGA (O.)**, « Les enjeux politiques de la publicité ciblée », *CNRS Le Journal*, 17 juin 2021, disponible en ligne : https://lejournal.cnrs.fr/billets/les-enjeux-de-la-publicite-politique-ciblee [consulté le 29 juillet 2021].

**GOYA (C.)**, « Cédric Villani dit que le RGPD n'aurait pas pu naître sans 'l'héroïsme' du lanceur d'alerte Edward Snowden », *Business Insider France*, 14 juin 2018, disponible en ligne : https://www.businessinsider.fr/cedric-villani-dit-que-le-rgpd-naurait-pas-pu-naitre-sans-lheroisme-du-lanceur-dalerte-edward-snowden-88078 [consulté le 1 août 2021].

**GRECO DE MARCO LEITE (G.), BOUGRINE (A.)**, « La nouvelle loi brésilienne sur la protection des données personnelles inspirée du RGPD européen », *UggcAvocats*, 18 juin 2019, disponible en ligne : https://www.uggc.com/la-nouvelle-loi-bresilienne-sur-la-protection-des-donnees-personnelles-inspiree-du-rgpd-europeen/ [consulté le 9 août 2021].

**- H -**

**HEAVEN (W. D.)**, « This has just become a big week for AI regulation », *MIT Technology Review*, 21 avril 2021, disponible en ligne : https://www.technologyreview.com/2021/04/21/1023254/ftc-eu-ai-regulation-bias-algorithms-civil-rights/ [consulté le 13 août 2021].

**HERN (A.)**, « Cambridge Analytica did work for Leave.EU, emails confirm », *The Guardian*, 30 juillet 2019, disponible en ligne : https://www.theguardian.com/uk-news/2019/jul/30/cambridge-analytica-did-work-for-leave-eu-emails-confirm [consulté le 28 juillet 2021].

**HUBERT (G.)**, reprise des propos de **ROUVROY (A.)**, « Algorithmes et responsabilités », *internetactu*, 16 mars 2016, disponible en ligne : https://www.internetactu.net/2016/03/16/algorithmes-et-responsabilites/ [consulté le 15 août 2021].

**- K -**

**KAHN (S.)**, « Des sénateurs américains veulent faire éclater les bulles de filtre », *Le Figaro*, 5 novembre 2019, disponible en ligne : https://www.lefigaro.fr/secteur/high-tech/des-senateurs-americains-veulent-faire-eclater-les-bulles-de-filtre-20191105 [consulté le 16 août 2021].

**KALLENBORN (G.)**, « Malade du SIDA, drogué, victime de viol… comment les publicitaires nous catégorisent », *01Net*, 28 janvier 2019, disponible en ligne : https://www.01net.com/actualites/malade-du-sida-drogue-victime-de-viol-comment-les-publicitaires-nous-categorisent-1621728.html, [consulté le 6 août 2021].

**KARAPINAR (O.)**, « Gabriel Weinberg : Faire éclater la bulle de filtrage », *Medium*, 16 novembre 2020, disponible en ligne : https://medium.com/essentiels/gabriel-weinberg-faire-%C3%A9clater-la-bulle-de-filtrage-9546d2ae826d [consulté le 16 août 2021].

**- L -**

**LA QUADRATURE DU NET**, « Amende de 746 millions d'euros contre Amazon suite à nos plaintes collectives », 30 juillet 2021, disponible en ligne : https://www.laquadrature.net/2021/07/30/amende-de-746-millions-deuros-contre-amazon-suite-a-nos-plaintes-collectives/ [consulté le 5 août 2021].

**LA QUADRATURE DU NET**, « Les GAFAM échappent au RGPD, la CNIL complice », 25 mai 2021, disponible en ligne : https://www.laquadrature.net/2021/05/25/les-gafam-echappent-au-rgpd-avec-la-complicite-de-la-cnil/ [consulté le 5 août 2021].

**LAUSSON (J.)**, « Jeu de go : victoire définitive 4 à 1 pour AlphaGo contre Lee Sedol », *Numerama*, 15 mars 2016, disponible en ligne : https://www.numerama.com/sciences/152345-jeu-de-go-victoire-definitive-4-a-1-pour-alphago-contre-lee-sedol.html [consulté le 27 juillet 2021].

**LE CALME (S.)**, « Commission européenne : Facebook, Google et Twitter ne respectent pas le code de conduite volontaire qu'ils ont signé pour combattre les fake news », *Developpez*, 1 mars 2019, disponible en ligne : https://www.developpez.com/actu/249130/Commission-

europeenne-Facebook-Google-et-Twitter-ne-respectent-pas-le-code-de-conduite-volontaire-qu-ils-ont-signe-pour-combattre-les-fake-news/ [consulté le 13 août 2021].

**LESAGE (N.)**, « Des universitaires vont étudier les chambres d'écho responsables de la toxicité de Twitter », *Numerama*, 31 juillet 2018, disponible en ligne : https://www.numerama.com/tech/402175-des-universitaires-vont-etudier-les-chambres-decho-responsables-de-la-toxicite-de-twitter.html [consulté le 28 juillet 2021].

**LEWIS (P.), HILDER (P.)**, « Leaked: Cambridge Analytica's blueprint for Trump victory », *The Guardian*, 23 mars 2018, disponible en ligne : https://www.theguardian.com/uk-news/2018/mar/23/leaked-cambridge-analyticas-blueprint-for-trump-victory [consulté le 28 juillet 2021].

**LUMB (D.)**, « Why Scientists Are Upset About The Facebook Filter Bubble Study », Fastcompany, 5 août 2015, disponible en ligne : https://www.fastcompany.com/3046111/why-scientists-are-upset-over-the-facebook-filter-bubble-study [consulté le 1 août 2021].

**- M -**

**MAXIMIM (N.)**, « Plateformes : la Commission européenne a ouvert une consultation sur le Digital Services Act », *Dalloz actualité IP/IT*, 8 juin 2020, disponible en ligne : https://www.dalloz-actualite.fr/flash/plateformes-commission-europeenne-ouvert-une-consultation-sur-digital-services-act, [consulté le 7 août 2021].

**- N -**

**NUNEZ (M.)**, « Facebook's Fight Against Fake News Was Undercut by Fear of Conservative Backlash », *Gizmodo*, 14 novembre 2016, [consulté le 11 août 2021].

**- P -**

**PARISER (E.)**, « Did Facebook's Big Study Kill My Filter Bubble Thesis? Not really — and here's why », *Wired*, 5 juillet 2015, disponible en ligne : https://www.wired.com/2015/05/did-facebooks-big-study-kill-my-filter-bubble-thesis/ [consulté le 1 août 2021].

**POILVE (B.)**, « Les enchères en temps réel (RTB), un système complexe », *Laboratoire d'innovation numérique de la CNIL*, 14 janvier 2020, disponible en ligne : https://linc.cnil.fr/fr/les-encheres-en-temps-reel-rtb-un-systeme-complexe [consulté le 6 août 2021].

**PREVOST (S.)**, « 2028 : procès du ranking social », *Dalloz actualité*, 13 janvier 2020, disponible en ligne : https://www.dalloz-actualite.fr/flash/2028-proces-du-ranking-social [consulté le 15 août 2021].

**- R -**

**RYAN (J.)**, « The ICO's failure to act on RTB, the largest data breach ever recorded in the UK », *Brave*, 17 janvier 2020, disponible en ligne : https://brave.com/ico-faces-action/ [consulté le 6 août 2021].

**RYAN (J.)**, « Update on GDPR complaint (RTB ad auctions) », *Brave*, 28 janvier 2019, disponible en ligne : https://brave.com/update-rtb-ad-auction-gdpr/ [consulté le 6 août 2021].

**- S -**

**SCHMITT (C.)**, « Sortez de votre bulle ! », *France24*, 19 octobre 2020, disponible en ligne : https://www.france24.com/fr/europe/20201019-sortez-de-votre-bulle [consulté le 16 août 2021].

**SEGOND (V.)**, « Des données personnelles très convoitées », *Le Monde*, 28 mai 2017, disponible en ligne : https://www.lemonde.fr/economie/article/2017/05/28/des-donnees-personnelles-tres-convoitees_5135092_3234.html [consulté le 29 juillet 2021].

**SHEARER (E.)**, « More than eight-in-ten Americans get news from digital devices », *Pew Research Center*, 12 janvier 2021, disponible en ligne : https://www.pewresearch.org/fact-tank/2021/01/12/more-than-eight-in-ten-americans-get-news-from-digital-devices/ [consulté le 27 juillet 2021].

**SIX (N.)**, « L'algorithme de recommandation de YouTube critiqué pour sa mise en avant de contenus extrêmes », *Le Monde*, 16 octobre 2019, disponible en ligne : https://www.lemonde.fr/pixels/article/2019/10/16/l-algorithme-de-recommandation-de-youtube-critique-pour-sa-mise-en-avant-de-contenus-extremes_6015784_4408996.html [consulté le 2 août 2021].

**- T -**

**TELLIER (M.)**, « La fracture numérique n'épargne pas les jeunes », *France culture*, 31 mai 2020, disponible en ligne : https://www.franceculture.fr/numerique/la-fracture-numerique-nepargne-pas-les-jeunes [consulté le 9 août 2021].

**TERRASSON (B.)**, « Google repousse la fin des cookies tiers à 2023 », *SiècleDigital*, 25 juin 2021, disponible en ligne : https://siecledigital.fr/2021/06/25/google-cookies-tiers/ [consulté le 17 août 2021].

**- U -**

**UNIVERSITÉ DU TEXAS À DALLAS**, « Recommended for you: Role, impact of tools behind automated product picks explored: Pros, cons of recommender systems. », *ScienceDaily*, 4 mars 2021, disponible en ligne : https://www.sciencedaily.com/releases/2021/03/210304145157.htm [consulté le 3 août 2021].

**- V -**

**VALLET (F.)**, « Oana Goga : « Facebook n'est pas compétent pour déterminer si une publicité est politique ou non » », *LINC*, 28 janvier 2021, disponible en ligne : https://linc.cnil.fr/fr/oana-goga-facebook-nest-pas-competent-pour-determiner-si-une-publicite-est-politique-ou-non [consulté le 17 août 2021].

**VESTAGER (M.)**, « Algorithms and democracy », *AlgorithmWatch Online Policy Dialogue*, 30 octobre 2020, disponible en ligne : https://ec.europa.eu/commission/commissioners/2019-2024/vestager/announcements/algorithms-and-democracy-algorithmwatch-online-policy-dialogue-30-october-2020_en [consulté le 2 août 2021].

**VITARD (A.)**, « Google accusé de saboter le Digital Services Act, Sundar Pichai s'excuse », *L'usine digitale*, 16 novembre 2020, disponible en ligne : https://www.usine-digitale.fr/editorial/google-accuse-de-saboter-le-digital-services-act-sundar-pichai-s-excuse.N1028599, [consulté le 8 aout 2021].

**VITKINE (B.)**, « La Russie en quête de « souveraineté » sur Internet », *Le monde*, 7 avril 2021, disponible en ligne : https://www.lemonde.fr/international/article/2021/04/07/la-russie-en-quete-de-souverainete-sur-internet_6075874_3210.html [consulté le 15 août 2021].

## VI. RAPPORTS, BILANS, DOCUMENTS

**- A -**

**ANSSI**, *Stratégie nationale pour la sécurité du numérique*, 16 octobre 2015, disponible en ligne : https://www.ssi.gouv.fr/actualite/la-strategie-nationale-pour-la-securite-du-numerique-une-reponse-aux-nouveaux-enjeux-des-usages-numeriques/ [consulté le 17 août 2021].

**AUTORITE DE LA CONCURRENCE**, *Avis n° 10-A-29 du 14 décembre 2010 sur le fonctionnement concurrentiel de la publicité en ligne*, disponible en ligne : https://www.autoritedelaconcurrence.fr/sites/default/files/commitments/10a29.pdf [consulté le 3 août 2021].

**AUTORITE DE LA CONCURRENCE, BUNDESKARTELLAMT**, *Algorithmes et concurrence*, novembre 2019, disponible en ligne : https://www.autoritedelaconcurrence.fr/sites/default/files/2020-03/algorithms-and-competition_fr.pdf [consulté le 2 août 2021].

**- B -**

**BEN-ISRAEL (I.), CERDIO (J.), EMA (A.)** et al., *Vers une régulation des systèmes d'IA*, CAHAI – Comité ad hoc sur l'intelligence artificielle, Conseil de l'Europe, 2020, 209 p., disponible en ligne : https://edoc.coe.int/fr/intelligence-artificielle/9652-vers-une-regulation-des-sytemes-d-ia.html [consulté le 9 août 2021].

**- C -**

**CABRERA BLAZQUEZ (F. J.), CAPPELLO (M.), RABIE (I.)** et al., *Le cadre juridique relatif aux plateformes de partage de vidéos*, IRIS Plus, Observatoire européen de l'audiovisuel, Strasbourg, 2018, p. 7, disponible en ligne : https://rm.coe.int/le-cadre-juridique-relatif-aux-plateformes-de-partage-de-videos/16808b05ef [consulté le 26 juillet 2021].

**CARDON (D.)**, *Évènement de lancement du cycle de débats publics sur les enjeux éthiques des algorithmes*, CNIL, 23 janvier 2017, disponible en ligne : https://www.cnil.fr/sites/default/files/atoms/files/compte_rendu_table-ronde_-_ethique_et_numerique_-_les_algorithmes_en_debat.pdf [consulté le 28 juillet 2021].

**CENTER FOR COUNTERING DIGITAL HATE**, *Malgorithm : how instagram's algorithm publishes misinformation and hate to millions during a pandemic*, 9 mars 2021, disponible en ligne : https://www.counterhate.com/malgorithm [consulté le 7 août 2021].

**CEDP, CONTR. EPD**, *Joint Opinion 5/2021 on the proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act)*, 18 juin 2021, disponible en ligne : https://www.dalloz-

actualite.fr/sites/dalloz-actualite.fr/files/resources/2021/07/avis_conjoint_cedp.pdf [consulté le 13 août 2021].

**CLAES (A.), WIARD (V.), MERCENIER (H.)** et al., « Algorithmes de recommandation et culture technique : penser le dialogue entre éducation et design », *Tic et société*, vol. 15 n° 1, pp. 127-157, https://journals.openedition.org/ticetsociete/5915 [Consulté le 4 aout 2021].

**CNDCH**, *Avis relatif à la lutte contre la haine en ligne*, (A - 2021 - 9), JORF n° 0170, 24 juillet 2021, disponible en ligne : https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000043851103 [consulté le 14 août 2021].

**CNIL**, *Comment permettre à l'Homme de garder la main ? Les enjeux éthiques des algorithmes et de l'intelligence artificielle*, Rapport de décembre 2017, disponible en ligne : https://www.cnil.fr/sites/default/files/atoms/files/cnil_rapport_garder_la_main_web.pdf [consulté le 25 juillet 2021].

**COMMISSION EUROPEENNE**, *Analyse d'impact accompagnant la proposition de règlement sur les services numériques*, SWD(2020) 348 final, 15 décembre 2020, disponible en ligne : https://digital-strategy.ec.europa.eu/en/library/impact-assessment-digital-services-act [consulté le 7 août 2021].

**COMMISSION EUROPEENNE**, *Antitrust: la Commission inflige une amende de 1,49 milliards d'euros à Google pour pratiques abusives en matière de publicité en ligne*, communiqué de presse, Bruxelles, 20 mars 2019, Disponible en ligne : https://ec.europa.eu/commission/presscorner/detail/fr/IP_19_1770 [consulté le 3 août 2021].

**COMMISSION EUROPEENNE**, *EU code of Practice on Disinformation*, septembre 2018, disponible en ligne : https://digital-strategy.ec.europa.eu/en/news/code-practice-disinformation [consulté le 12 août 2021].

**COMMISSION EUROPEENNE**, *Façonner l'avenir numérique de l'Europe*, communication de la Commission au Parlement européen, au Conseil, au Comité économique et social européen et au Comité des régions, COM(2020) 67 final, 19 février 2020, 17 p., disponible en ligne : https://ec.europa.eu/info/sites/default/files/communication-shaping-europes-digital-future-feb2020_fr.pdf [consulté le 7 août 2021].

**COMMISSION EUROPEENNE**, *Lutter contre la désinformation en ligne: une approche européenne*, Communication de la Commission au Parlement européen, au Conseil, au Comité économique et social européen et au Comité des régions, COM/2018/236 final, disponible en ligne : https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX%3A52018DC0236 [consulté le 11 août 2021].

**COMMISSION EUROPEENNE POUR LA DEMOCRATIE PAR LE DROIT (COMMISSION DE VENISE)**, *Rapport sur le calendrier et l'inventaire des critères politiques d'évaluation d'une élection* [en ligne], CDL-AD(2010)037, Strasbourg, 21 octobre 2010, p. 5, [consulté le 4 août 2021].

**CONSEIL D'ÉTAT**, *Le numérique et les droits fondamentaux*, 9 septembre 2014, disponible en ligne : https://www.conseil-etat.fr/actualites/actualites/le-numerique-et-les-droits-fondamentaux [consulté le 15 août 2021].

**CONSEIL DE L'EUROPE**, *Algorithmes et droits humains*, étude du Conseil de l'Europe DGI(2017)12, 2017, disponible en ligne : https://rm.coe.int/algorithms-and-human-rights-fr/1680795681 [consulté le 29 juillet 2021].

**CONSEIL DE L'EUROPE**, *Intelligence artificielle et protection des données : enjeux et solutions possibles*, T-PD(2018)09Rev, Strasbourg, 25 janvier 2019, p. 8, disponible en ligne : https://rm.coe.int/intelligence-artificielle-et-protection-des-donnees-enjeux-et-solution/168091f8a5 [consulté le 7 août 2021].

**CONSEIL DE L'EUROPE**, *Recommandation CM/Rec(2018)11 du Comité des Ministres aux États membres sur le pluralisme des médias et la transparence de leur propriété*, 7 mars 2018, disponible en ligne : https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680790e36 [consulté le 3 août 2021].

**CONSEIL DE L'EUROPE**, *Recommandation CM/Rec(2020)1 du Comité des Ministres aux États membres sur les impacts des systèmes algorithmiques sur les droits de l'homme*, 8 avril 2020, disponible en ligne : https://search.coe.int/cm/pages/result_details.aspx?ObjectId=09000016809e1124 [consulté le 29 juillet 2021].

**CONSEIL NATIONAL DU NUMERIQUE**, *Avis n°2015-3 relatif au projet de loi pour une République numérique*, 30 novembre 2015, disponible en ligne : https://cnnumerique.fr/files/2017-10/Avis-du-CNNum-sur-le-projet-de-loi-numerique.pdf [consulté le 2 aout 2021].

**CONSEIL SUPERIEUR DE L'AUDIOVISUEL**, *Capacité à informer des algorithmes de recommandation : Une expérience sur le service Youtube*, Rapport de novembre 2019, disponible en ligne : https://www.csa.fr/Informer/Collections-du-CSA/Focus-Toutes-les-etudes-et-les-comptes-rendus-synthetiques-proposant-un-zoom-sur-un-sujet-d-actualite/Capacite-a-informer-des-algorithmes-de-recommandation-une-experience-sur-le-service-YouTube-2019 [consulté le 26 juillet 2021].

**CONTROLEUR EUROPEEN DE LA PROTECTION DES DONNEES**, *Avis du CEPD sur la manipulation en ligne et les données à caractère personnel*, avis n° 3/2018, 19 mars 2018, disponible en ligne : https://edps.europa.eu/sites/edp/files/publication/18-03-19_opinion_online_manipulation_fr.pdf [consulté le 1 août 2021].

**CONTROLEUR EUROPEEN DE LA PROTECTION DES DONNEES**, *Avis n° 01/2021 concernant la proposition de législation sur les services numériques,* , 10 février 2021, disponible en ligne : https://edps.europa.eu/data-protection/our-work/publications/avis-du-cepd/digital-services-act_fr [consulté le 8 août 2021].

**CSA**, *La propagation des fausses informations sur les réseaux sociaux : Étude du service Twitter*, novembre 2020, disponible en ligne : https://www.csa.fr/Informer/Collections-du-CSA/Focus-Toutes-les-etudes-et-les-comptes-rendus-synthetiques-proposant-un-zoom-sur-un-sujet-d-actualite/La-propagation-des-fausses-informations-sur-les-reseaux-sociaux-etude-de-la-plateforme-Twitter [consulté le 12 août 2021].

**CSA**, *Lutte contre la diffusion de fausses informations sur les plateformes en ligne : bilan de l'application et de l'effectivité des mesures mises en œuvre par les opérateurs en 2019*, juillet 2020, disponible en ligne : https://www.vie-publique.fr/sites/default/files/rapport/pdf/275995.pdf [consulté le 11 août 2021].

**- D -**

**DE GANAY (C.), GILLOT (D.)**, *Pour une intelligence artificielle maîtrisée, utile et démystifiée*, Sénat, rapport d'information n° 464, 15 mars 2017, disponible en ligne : http://www.senat.fr/rap/r16-464-1/r16-464-11.html#toc1 [consulté le 27 juillet 2021].

**- E -**

**ESLAMI (M.), RICKMAN (A.), VACCARO (K.)**, « "I always assumed that I wasn't really that close to [her]": Reasoning about invisible algorithms in the news feed », *CHI '15: Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems*, avril 2015, pp. 153-162, disponible en ligne : http://www-personal.umich.edu/~csandvig/research/Eslami_Algorithms_CHI15.pdf [consulté le 17 août 2017].

**- F -**

**FAURE-MITIAN (V.), FASQUELLE (D.)**, *Rapport d'information sur les plateformes numériques* [en ligne], Assemblée Nationale, 24 juin 2020, [consulté le 16 août 2021].

**- G -**

**GROUPE DE TRAVAIL « ARTICLE 29 » SUR LA PROTECTION DES DONNEES**, *Avis 05/2014 sur les Techniques d'anonymisation*, 10 avril 2014, disponible en ligne : https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_fr.pdf [consulté le 9 août 2021].

**- I -**

**INSTITUT FRANÇAIS D'OPINION PUBLIQUE**, *Enquête sur le complotisme – vague 2*, sondage IFOP pour la Fondation Jean-Jaurès et Conspiracy Watch, janvier 2019, disponible en ligne : https://www.ifop.com/wp-content/uploads/2019/02/115960-Pr%C3%A9sentation-version-publi%C3%A9e.pdf [consulté le 26 juillet 2021].

**- M -**

**MOZILLA**, *YouTube Regrets : A crowdsourced investigation into YouTube's recommendation algorithm*, juillet 2021, disponible en ligne : https://assets.mofoprod.net/network/documents/Mozilla_YouTube_Regrets_Report.pdf [consulté le 11 août 2021].

**- P -**

**POUILLET (Y.), FRENAY (B.)**, Comité consultatif de la convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, Conseil de l'europe, T-PD(2019)07, Strasbourg, 9 septembre 2019, disponible en ligne : https://rm.coe.int/rapport-et-propositions-de-recommandations-sur-le-profilage-et-la-conv/1680973672 [consulté le 2 août 2021].

**PARLEMENT EUROPEEN**, *Un régime de responsabilité civile pour l'intelligence artificielle,* 20 octobre 2020, disponible en ligne : https://www.europarl.europa.eu/doceo/document/TA-9-2020-0276_FR.html [consulté le 16 août 2021].

**- S -**

**SENAT**, *Avis politique sur la désinformation en ligne et les atteintes aux processus électoraux*, Paris, 18 mars 2021, disponible en ligne : http://www.senat.fr/fileadmin/Fichiers/Images/commission/affaires_europeennes/avis_politiques/AP_desinformation_PASTILLE.pdf [consulté le 3 août 2021].

**SENAT**, *L'illectronisme ne disparaîtra pas d'un coup de tablette magique !*, rapport du Sénat pour la mission d'information sur l'inclusion numérique, 17 septembre 2020, disponible en ligne : https://www.senat.fr/rap/r19-711/r19-7112.html [consulté le 9 août 2021].

**- V -**

**VILLANI (C.)**, *Donner un sens à l'intelligence artificielle : pour une stratégie nationale et européenne*, rapport de mission parlementaire, 28 mars 2018, disponible en ligne : https://www.vie-publique.fr/sites/default/files/rapport/pdf/184000159.pdf [consulté le 27 juillet 2021].

**- W -**

**WAGNER (B.)**, Étude sur les dimensions des droits humains dans les techniques de traitement automatisé des données (en particulier les algorithmes) et éventuelles implications réglementaires, Conseil de l'Europe, Comité d'experts sur les intermédiaires d'internet (MSI-NET), 6 octobre 2017. Disponible sur https://rm.coe.int/algorithmes-et-droits-humains-etude-sur-les-dimensions-des-droitshuma/1680796d11 [consulté le 7 août 2021].

**WE ARE SOCIAL**, Digital 2021 global overview report, janvier 2021, disponible en ligne : https://wearesocial-net.s3-eu-west-1.amazonaws.com/wp-content/uploads/common/reports/digital-2021/digital-2021-global.pdf [consulté le 27 juillet 2021].

**WOLLEY (S.), HOWARD (P.)**, Computational Propaganda Worldwide: Executive Summary, rapport du Computational propaganda Research Project, novembre 2017, disponible en ligne : https://demtech.oii.ox.ac.uk/wp-content/uploads/sites/89/2017/06/Casestudies-ExecutiveSummary.pdf [consulté le 3 août 2021].

## VII. BLOGS, SITES, AUTRES

**- A -**

**ALGOTRANSPARENCY**, disponible en ligne : https://www.algotransparency.org/ [consulté le 17 août 2021].

**- C -**

**CHAOUCHE (Y.)**, « Identifiez les différents types d'apprentissage automatiques », *formation Openclassrooms*, 2021, disponible en ligne : https://openclassrooms.com/fr/courses/4011851-initiez-vous-au-machine-learning/4020611-identifiez-les-differents-types-dapprentissage-automatiques [consulté le 27 juillet 2021].

**- I -**

**INTERNET LIVE STATS**, 2021, disponible en ligne : https://www.internetlivestats.com/ [consulté le 27 juillet 2021].

**- L -**

**LOBBYPLAG**, aperçu des 3132 amendements déposés sur le RGPD, disponible en ligne : https://lobbyplag.eu/map [consulté le 14 août 2021].

**- P -**

**POLITIQUE DE CONFIDENTIALITE DE GOOGLE**, « Proposer des services personnalisés, notamment en matière de contenu et d'annonces », mise à jour au 1er juillet 2021, disponible en ligne : https://policies.google.com/privacy?hl=fr&fg=1, [consulté le 6 août 2021].

**- R -**

**ROPARS (F.)**, « SEO : les taux de clics et les performances des liens selon la position dans les SERPs », *Blog du modérateur*, 28 août 2019, disponible en ligne : https://www.blogdumoderateur.com/etude-taux-de-clics-et-les-performances-des-liens-selon-la-position-dans-les-serps/ [consulté le 3 août 2021].

**- T -**

**TREGUER (F.)**, « réclamation contre Google », *La Quadrature du Net*, 28 mai 2018, disponible en ligne : https://gafam.laquadrature.net/wp-content/uploads/sites/9/2018/05/google.pdf [consulté le 5 août 2021].

**- W -**

**WEBRANKINFO**, « Encyclopédie Google : produits, services, brevets… », disponible en ligne : https://www.webrankinfo.com/google [consulté le 8 août 2021].

**- Y -**

**YOUTUBE**, « Officiel DEFAKATOR », disponible en ligne : https://www.youtube.com/channel/UCU0FhLr6fr7U9GOn6OiQHpQ [consulté le 17 août 2021].

# TABLE DE JURISPRUDENCES

## COMMISSION EUROPEENNE

Commission européenne, 24 mars 2004, *Microsoft*, aff. C-3/37.792.

Commission européenne, 18 juillet 2018, *Google Android*, aff. AT.40099.

Commission européenne, 20 mars 2019, *Google Search (AdSense)*, aff. AT.40411.

## COUR DE JUSTICE DE L'UNION EUROPEENNE

CJCE, 14 février 1978, United Brands et United Brands Continentaal c/ Commission, aff. C-27/76.

CJCE, 6 ch., 26 novembre 1998, Oscar Bronner GmbH & Co. KG c. Mediaprint Zeitungs, aff. C-7/97.

CJUE, 2 mai 2012, *SAS Institute Inc. v. World Programming Ltd*., aff. C-406/10.

CJUE, 29 juillet 2019, *Fashion ID GmbH & Co. KG*, aff. C-40/17.

CJUE, 1 octobre 2019, *Verbraucherzentrale Bundesverband eV c/ Planet49 GmbH*, Aff. C-673/17.

## CONSEIL CONSTITUTIONNEL

Cons. const., 11 octobre 1984, n° 84-181 DC.

Cons. const., 18 septembre 1986, n° 86-217 DC.

Cons. const., 10 juin 2004, n° 2004-496 DC.

Cons. const., 8 décembre 2017, n° 2017-5026 AN.

Cons. const., 20 décembre 2018, n° 2018-773 DC.

Cons. const., 18 juin 2020, n° 2020-801 DC.

## COUR CONSTITUTIONNELLE ALLEMANDE

Bundesverfassungsgerichts 65,1, *Volkszählung*, 15 décembre 1983.

## CONSEIL D'ÉTAT

CE, 13 février 2009, *Élections municipales de la commune de Fuveau*, n° 317637.

CE, 8 février 2017, *JCDecaux France*, n° 393714.

CE, 19 juillet 2017, *Google Inc.*, n° 399922.

CE, 19 juin 2020, *Association des agences-conseils en communication et autres*, n° 434684.

## COUR DE CASSATION

Cass. 1e. civ., 18 octobre 2017, n° 16-19.740.

## TRIBUNAL DE GRANDE INSTANCE

TGI Paris, 18 décembre 2007, *J.-Y. Lafesse et a. c/ Dailymotion*, n° 06/18289.

TGI Brest, 11 juin 2013, *Josette B. / Catherine L., SAS-Overblog.*

TGI Versailles, 26 février 2019, *Association des Juristes pour l'Enfance / OVH et Subrogalia SL*., n° 16/07633.

TGI Paris, 17 mai 2019, *Marie-Pierre Vieu et Pierre Ouzoulias c/ Twitter et Christophe Castaner*, n° RG 19/53935.

## CNIL

CNIL, 21 janvier 2019, délibération n°SAN-2019-001.

# TABLE DES NORMES

## ARTICLES

## REGLEMENTS

Proposition de Règlement du parlement européen et du Conseil établissant des règles harmonisées concernant l'intelligence artificielle (législation sur l'intelligence artificielle) et modifiant certains actes législatifs de l'Union, COM (2021) 206 final, 21 avril 2021.

Proposition de règlement du Parlement européen et du Conseil relatif à un marché intérieur des services numériques (Législation sur les services numériques) et modifiant la directive 2000/31/CE.

Proposition de règlement du Parlement européen et du Conseil relatif aux marchés contestables et équitables dans le secteur numérique (législation sur les marchés numériques).

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

## DIRECTIVES

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 («*directive sur le commerce électronique*»).

## LOIS

Loi fondamentale pour la République fédérale d'Allemagne du 23 mai 1949.

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

Loi n° 86-1067 du 30 septembre 1986 relative à la liberté de communication.

Loi n° 95-101 du 2 février 1995 relative au renforcement de la protection de l'environnement.

Loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique.

Loi constitutionnelle n° 2005-205 du 1er mars 2005 relative à la Charte de l'environnement.

Loi n° 2018-1201 du 22 décembre 2018 relative à la lutte contre la manipulation de l'information.

Loi n° 2018-1202 du 22 décembre 2018 relative à la lutte contre la manipulation de l'information.

S. 2763, 116th Congress, Filter Bubble Transparency Act, 31 octobre 2019.

Loi n° 2020-766 du 24 juin 2020 visant à lutter contre les contenus haineux sur internet.

# INDEX

## *A*



## *B*



## *C*



## *D*



## *E*



## *F*

## *G*



## *H*



## *I*



## *K*



## *L*



## *M*



## *N*



## *O*



## *P*



## *Q*

## *R*



## *S*



## *T*



## *V*



## *Y*

# TABLE DES MATIERES