Introduction au droit du commerce électronique

➢ Définition du commerce électronique

Dans la directive du 8 juin 2000 sur le commerce électronique, il n'y a pas de vraie définition du commerce électronique.

L'un des principaux objectifs de cette directive a été d'établir des cas d'exemption de responsabilité au profit de certains prestataires de service d'internet jouant un (simple) rôle d'intermédiaire.

La LCEN du 21 juin 2004 dite Loi de Confiance dans l'Economie numérique, qui a transposé cette directive en droit français, donne une définition assez large en définissant le commerce électronique comme étant **l'échange d'information par voie électronique.**

La Directive de juin 2000 concernant le commerce électronique a donc été transposée en France par la loi du 21 juin 2004 dite LCEN.

Elle prévoit notamment :

- **une protection du consommateur par l'obligation d'information pour le vendeur en ligne de s'identifier sur le site sous peine de sanctions.**

- **La responsabilité des intermédiaires techniques de l'Internet qu'ils soient fournisseurs d'accès, hébergeurs de site) ou encore des éditeurs de services (anonymes ou professionnels).**

Depuis une Directive de 1999 sur la signature électronique, l'écrit électronique a la même valeur que l'écrit papier. Cette Directive a été Introduite en France par la loi du 31 mars 2000.

En pratique, la signature sécurisée se heurte à des difficultés techniques de mise en place de certification.

Les autres raisons du très fort développement du commerce électronique tiennent dans la démocratisation progressive de l'Internet haut débit (ADSL), qui couvre la quasi-totalité du territoire français.

Il convient de s'arrêter précisément sur les dispositions issues de la LCEN du 21 juin 2004.

➢ La responsabilité des prestataires techniques du commerce électronique

Les dispositions prévues dans la Loi de Confiance dans l'Economie Numérique

La communication au public en ligne, également appelée communication sur internet, est une des formes des communications électroniques.

L'article 1er de la loi n° 86-1067 du 30 septembre 1986 relative à la liberté de communication, modifié par ladite **Loi de Confiance dans l'Economie Numérique ou LCEN**, et l'article 1er de cette même loi posent qu' « *on entend par communication au public par voie électronique toute mise à disposition du public ou de catégories de public, par un procédé de communication électronique, de signes, de signaux, d'écrits, d'images ou de messages de toute nature qui n'ont pas le caractère d'une correspondance privée* ».

Il existe plusieurs acteurs du commerce électronique auxquels s'appliquent des obligations diverses et variées.

Les intermédiaires techniques qu'ils soient fournisseurs d'accès, fournisseurs d'hébergement ou éditeurs de services se voient imposer quelques obligations spécifiques destinées notamment à permettre leur identification en vue de la mise en jeu de leur éventuelle responsabilité en cas d'infraction constatée.

Quid des éditeurs de services et des intermédiaires techniques ?

La communication au public en ligne relève donc de deux formes de services ou d'activités :

1. **Les éditeurs de services**
2. **Les intermédiaires techniques**

1) Les éditeurs de services

Les éditeurs de services peuvent être de deux types.

Il s'agit soit d'éditeurs professionnels soit d'éditeurs non professionnels.

Afin notamment de permettre la mise en jeu de leur éventuelle responsabilité, la loi impose aux éditeurs de services (*que l'on peut considérer comme étant les exploitants de sites, responsables des contenus rendus accessibles sur internet*) de satisfaire à certaines obligations de transparence en fournissant quelques informations sur eux-mêmes. L'importance des contraintes diffère selon qu'ils agissent en tant que professionnels ou non.

Les éditeurs professionnels auront plus d'informations à fournir que les non professionnels.

- **Éditeurs de services professionnels (mentions légales)**

L'article 6-III-1 de la loi du 21 juin 2004 pose, à cet égard, que « les personnes dont l'activité est d'éditer », à titre professionnel, « un service de communication au public en ligne » se doivent de mettre à disposition du public (des internautes) :

a) s'il s'agit de personnes physiques :

- leurs nom, prénoms, domicile et numéro de téléphone et, si elles sont assujetties aux formalités d'inscription au registre du commerce et des sociétés ou au répertoire des métiers, le numéro de leur inscription
- le nom du directeur ou du codirecteur de la publication et, le cas échéant, celui du responsable de la rédaction au sens de l'article 93-2 de la loi n° 82-652 du 29 juillet 1982" (...) ; "
- le nom, la dénomination ou la raison sociale, l'adresse et le numéro de téléphone de leur fournisseur d'hébergement.

b) s'il s'agit de personnes morales (cf. associations ou sociétés) :
- leur dénomination ou leur raison sociale et leur siège social, leur numéro de téléphone et, s'il s'agit d'entreprises assujetties aux formalités d'inscription au registre du commerce et des sociétés ou au répertoire des métiers, le numéro de leur inscription, leur capital social, l'adresse de leur siège social ;
- le nom du directeur ou du codirecteur de la publication et, le cas échéant, celui du responsable de la rédaction au sens de l'article 93-2 de la loi n° 82-652 du 29 juillet 1982" (...) ; "
- le nom, la dénomination ou la raison sociale et l'adresse et le numéro de téléphone

de leur fournisseur d'hébergement.

➢ **Éditeurs de services non professionnels (mentions légales)**

L'article 6-III-2 de la même loi pose que « *les personnes éditant à titre non professionnel un service de communication au public en ligne peuvent ne tenir à la disposition du public, pour préserver leur anonymat, que le nom, la dénomination ou la raison sociale* » de leur fournisseur d'hébergement, « *sous réserve de lui avoir communiqué les éléments d'identification personnelle* » exigés des éditeurs de services agissant à titre professionnel.

L'éditeur de service non professionnel peut donc rester complètement anonyme vis-à-vis de ses visiteurs (et notamment ne pas désigner non plus de directeur de publication), mais il devra donner à son hébergeur les éléments d'identification (mentions légales) que l'on exige d'un éditeur de service professionnel.

➢ **Sanction du non-respect de l'obligation de transparence**

Le non-respect de ces obligations est, par l'article 6-VI-2 de la même loi, « *puni d'un an d'emprisonnement et de 75 000 euros d'amende* ». S'il s'agit de personnes morales, elles peuvent se voir appliquer les dispositions des articles L. 131-38 et L. 131-39 du Code pénal, comportant l'interdiction d'exercer cette activité "pour une durée de cinq ans au plus".

En l'état actuel de notre droit, les services de radio (webradios) et de télévision qui n'utilisent que ce mode de communication au public en ligne échappent aux dispositions de la loi du 30 septembre 1986, constitutives du statut des entreprises de communication audiovisuelle, et au contrôle du Conseil supérieur de l'audiovisuel (CSA).

2) Les intermédiaires techniques

Les intermédiaires techniques peuvent être de deux types, même si certains assument, en réalité, les deux fonctions. Ils sont dits « fournisseurs d'accès » ou « fournisseurs d'hébergement ».

L'article 6-I de la loi du 21 juin 2004 définit les « *fournisseurs d'accès* » comme « *les personnes dont l'activité est d'offrir un accès à des services de communication au public en ligne* ».

Les « fournisseurs d'hébergement » sont ceux qui assurent, « *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 service*s ».

➢ **Les fournisseurs d'accès**

L'article 6-I-1 de la loi du 21 juin 2004 impose, aux fournisseurs d'accès à l'internet, l'obligation d'informer « *leurs abonnés de l'existence de moyens techniques*

permettant de restreindre l'accès à certains services ou de les sélectionner" et de leur proposer « au moins un de ces moyens ».

Il s'agit, par des moyens techniques appropriés, de permettre le contrôle parental de l'accès à certains sites considérés comme peu conformes, pour des raisons de moralité notamment, aux contenus avec lesquels des enfants et des adolescents peuvent être mis en contact. Dès lors qu'ils satisfont à cette exigence, les fournisseurs d'accès échappent pratiquement à toute mise en jeu de leur responsabilité du fait du contenu des messages qui circulent sur les réseaux.

- **Les fournisseurs d'hébergement**

Les dispositions de l'article 6-I-2 et 6-I-3 de la loi du 21 juin 2004 concernant les fournisseurs d'hébergement sont quasiment exclusivement relatives aux conditions, très restrictives ou exceptionnelles, de la possible mise en jeu de leur responsabilité. Elles seront donc évoquées ci-dessous dans les développements consacrés à cette question.

L'article 6-II de la même loi de juin 2004 fait obligation aux intermédiaires techniques de détenir et de conserver « les données de nature à permettre l'identification de quiconque a contribué à la création du contenu ou de l'un des contenus des services » dont ils sont prestataires.

La directive de 2000 et la LCEN du 21 juin 2004 permettent aux Etats membres d'imposer à ces prestataires, une obligation de collaboration avec les autorités judiciaires ou les ayants droit en les informant promptement d'activités illicites alléguées.

La loi du 21 juin 2004 détermine désormais les conditions de mise en jeu de la responsabilité des divers acteurs de la communication au public en ligne.

La responsabilité des différents acteurs de l'internet

Conformément aux principes énoncés par la directive européenne du 8 juin 2000 sur le commerce électronique, la loi du 21 juin 2004 détermine désormais, de façon très restrictive, les conditions de l'éventuelle mise en jeu de la responsabilité civile et pénale des intermédiaires techniques.

1. La responsabilité des éditeurs de services

➢ Qualité et responsabilité d'un éditeur de services

Un éditeur de services est par définition l'exploitant d'un site internet. C'est celui qui prend la charge de la diffusion du contenu en éditant et en sélectionnant ledit contenu.

Le principe veut que tout exploitant de site sur le réseau internet est présumé responsable des textes et des informations qui y circulent (TGI Paris, 17e ch., 31 oct. 2002, M. c/ Licra : Légipresse 2002, n° 197, I, p. 16).

Un éditeur de site professionnel comme « Le Monde » peut voir sa responsabilité de directeur de publication directement engagée du fait de propos qu'il aura choisi de publier sur le site qu'il édite.

Quand le site est édité par un groupe de personnes, la personne qui est légalement condamnable est le directeur de publication.

➢ L'obligation de désigner un directeur de publication

Comme tout « *service de communication au public par voie électronique* », les services de communication au public en ligne, et plus précisément les éditeurs de services (ou sites internet), sont, aux termes de l'article 93-2 de la loi du 29 juillet 1982 modifié par la loi du 21 juin 2004, tenus d'avoir un directeur ou un codirecteur de la publication.

Chaque site internet se doit donc de désigner, sauf les cas d'un site internet non professionnel, un directeur ou un co-directeur de publication. Cela permettra à ceux qui se prétendent victime des contenus y figurant d'avoir le nom de celui qui endosse la responsabilité des propos et contenus figurant sur ledit site.

Le directeur de la publication étant considéré, par la loi, comme responsable, à titre d'auteur principal, de l'infraction, celui qui a formulé les propos ou rédigé les écrits litigieux (diffamatoires ou injurieux) doit être qualifié de complice et peut être poursuivi à ce titre.

2. La responsabilité des intermédiaires techniques

Distinction avec les producteurs

Pour les faire échapper à la mise en jeu de leur responsabilité, l'article 6-I-6 de la loi

du 21 juin 2004 pose que les intermédiaires techniques (fournisseurs d'accès et fournisseurs d'hébergement) « *ne sont pas des producteurs au sens de l'article 93-3 » de la loi « du 29 juillet 1982* ».

Ils ne produisent pas de contenu et ne servent que d'intermédiaires techniques dans la communication au public en ligne desdits contenus.

Parmi les intermédiaires techniques, on distingue la responsabilité des fournisseurs d'accès de celles des fournisseurs d'hébergement.

- **Fournisseurs d'accès**

Les fournisseurs d'accès, comme tous ceux qui, dans le secteur des communications électroniques, assument des activités techniques de transport ou de mise à disposition de messages ou de programmes, échappent, en principe, au nom de la neutralité des techniques et pour garantir la liberté d'expression, à toute mise en jeu de leur responsabilité du fait des contenus ainsi rendus accessibles.

- **Fournisseurs d'hébergement**

La directive de 2000 et la loi de confiance dans l'économie numérique qui la transpose n'imposent aux hébergeurs aucune obligation générale de surveillance des informations stockées ou transmises ni de recherche active de possibles activités illicites.

L'intervention des hébergeurs peut donc rester ponctuelle et bien délimitée sans que leur responsabilité ne puisse être engagée. L'hébergeur peut même choisir de ne pas surveiller de manière permanente et active les réseaux qu'il met à disposition de ses utilisateurs.

Compte tenu notamment de l'absence d'obligation générale de surveillance, les fournisseurs d'hébergement ne peuvent voir leur responsabilité engagée que dans les conditions restrictives que détermine, en des termes pratiquement identiques qu'il s'agisse de responsabilité civile ou pénale, l'article 6-I -2 de la loi du 21 juin 2004.

La mise en jeu de la responsabilité de l'hébergeur : L'obligation de notification préalable des contenus illicites

Principe :

Un hébergeur, quel qu'il soit, est donc, par principe, irresponsable des contenus qu'il héberge.

Exception :

L'article 6-I-2 de la loi de juin 2004 pose que ces intermédiaires techniques « ne peuvent voir leur responsabilité civile engagée du fait des activités ou des informations stockées » s'ils « *n'avaient pas effectivement connaissance de leur caractère illicite ou de faits et circonstances faisant apprécier ce caractère ou si, dès le moment où (ils) en ont eu cette connaissance, (ils) ont agi promptement pour*

retirer ces données ou en rendre l'accès impossible ».

Le même article précise cependant que cette quasi irresponsabilité de principe des fournisseurs d'hébergement ne vaut pas lorsque l'éditeur de services « agit sous (leur) autorité ou (leur) contrôle ».

La notification de contenus illicites ou comment demander la suppression d'un contenu ?

L'hébergeur étant irresponsable par principe des contenus (même) illicites qu'il héberge, il faudra, pour pouvoir prétendre engager valablement sa responsabilité et plus précisément pour qu'il s'estime tenu de retirer ledit contenu, respecter strictement les dispositions de l'article 6-I-5 dans le courrier qu'on sera amené à lui adresser.

L'article 6-I-5 de cette loi de juin 2004 précise que :

« *la connaissance des faits litigieux est présumée acquise »,* par les fournisseurs d'hébergement, lorsque leur sont communiqués les éléments suivants :

1. l**a date de la notification** (*dans le mail ou dans le courrier que l'on adresse à l'hébergeur)*

2. **si le notifiant est une personne physique :** il conviendra d'indiquer ses nom, prénoms, profession, domicile, nationalité, date et lieu de naissance ;
   si le requérant est une personne morale (société, association) : sa forme, sa dénomination, son siège social et l'organe qui la représente légalement ; les nom et domicile du destinataire" (ce qui, en l'espèce, semble vouloir maladroitement signifier l'éditeur du service et non le public ou le lecteur ou l'utilisateur final)

3. **les nom et domicile du destinataire ou, s'il s'agit d'une personne morale, sa dénomination et son siège social ;**
4. **la description des faits litigieux et leur localisation précise ;** *(le lien hypertexte menant au contenu litigieux)*

5. **les motifs pour lesquels le contenu doit être retiré, comprenant la mention des dispositions légales et des justifications de faits** *(il faudra donc être en mesure d'expliquer quelles sont les dispositions légales et les textes précis qui sanctionnent le contenu litigieux et justifient qu'il soit retiré ou modifié par l'hébergeur).*

6. l**a copie de la correspondance adressée à l'auteur** ou à l'éditeur des informations ou activités litigieuses demandant leur interruption, leur retrait ou leur modification, ou la justification de ce que l'auteur ou l'éditeur n'a pu être contacté ». *(l'hébergeur ne peut, en effet, être contacté qu'à titre subsidiaire cf. que parce que l'auteur, préalablement contacté, n'a pas souhaité obtempérer).*

Il est impératif de respecter strictement les conditions de forme et de fond prévues

par la loi pour la confiance dans l'économie numérique du 21 juin 2004 en son article 6-I-5.

A titre d'exemple, de nombreuses décisions ont vu une plateforme de blog (cf. overblog) gagner des procès visant à engager leur responsabilité en tant qu'hébergeur n'ayant pas souhaité retirer promptement des contenus illicites qui lui avait été notifiés au motif qu'elle avait pu démontrer, lors du procès, que la copie de la correspondance adressée à l'auteur ne figurait pas dans les notifications de contenus illicites qui lui avait été transmises.

Parce que le principe de la LCEN veut que l'hébergeur ne doive et ne puisse être contacté qu'à titre subsidiaire, ce dernier pouvait valablement considérer ne pas avoir à se conformer à la notification de contenu illicite qu'on lui avait transmise, faute pour cette dernière d'avoir respecté le cadre prévu par la loi.

A noter que l'hébergeur restera néanmoins tenu de retirer immédiatement les contenus dits **sensibles ou odieux** au sens de l'article 6-I-7 alinéas 3 et 4 de la LCEN parmi lesquels ceux ayant trait à l'incitation à la haine raciale, à la pornographie enfantine, à l'apologie des crimes contre l'humanité, à l'incitation à la violence et aux atteintes à la dignité humaine.

Ce type de contenus n'a même pas à lui être notifié ; ils devront être retirés spontanément par l'hébergeur.

La LCEN oblige cependant l'hébergeur à mettre en place un dispositif facilement accessible et visible permettant à toute personne de porter à leur connaissance ce type de données sensibles ou odieuses.

Les hébergeurs ont également l'obligation, d'une part, d'informer promptement les autorités publiques compétentes de toutes activités illicites de ce type qu'exerceraient les destinataires de leurs services, et, d'autre part, de rendre publics les moyens qu'elles consacrent à la lutte contre ces activités illicites.

Limites : Sanction des dénonciations abusives de contenus illicites

Au nom de la garantie de la liberté d'expression, ou pour limiter encore davantage la possibilité qu'un fournisseur d'hébergement ait connaissance de contenus illicites et puisse ainsi voir sa responsabilité engagée s'il n'agit pas « *promptement pour retirer ces informations ou en rendre l'accès impossible* », l'article 6-I-4 de la loi du 21 juin 2004 réprime *« le fait, pour toute personne, de présenter* », à un fournisseur d'hébergement, « *un contenu ou une activité comme étant illicite dans le but d'en obtenir le retrait ou d'en faire cesser la diffusion, alors qu'elle sait cette information inexacte* ».

La notification abusive est puni d'une peine pouvant aller jusqu'à un an d'emprisonnement et jusqu'à 15.000 euros d'amende.

Fiche pratique concernant la responsabilité des intermédiaires techniques

Comment doit-on se constituer la preuve d'une infraction commise sur internet ?

A titre préalable, il convient d'indiquer que lorsqu'une infraction est commise à votre encontre sur internet, le premier réflexe à avoir est avant tout de se ménager la preuve de la publication litigieuse.

Tout type de preuve peut être recueilli par l'entreprise (capture d'écran, impressions...), toutefois, en cas d'action en justice, il conviendra de respecter les règles de preuve applicables en fonction de l'action envisagée et notamment le principe de la loyauté de la preuve qui empêche que des informations soient obtenues de manière déloyale.

En effet, dans certains cas, un formalisme très strict doit être respecté pour constater le contenu litigieux faute de quoi la preuve pourrait ne pas être admise par le juge. Dans une décision du 10 avril 2013, le Tribunal de grande instance de Paris a ainsi considéré qu'une capture d'écran n'était pas suffisante pour établir la réalité d'une publication sur internet. C'est pourquoi il peut être recommandé de faire appel à un huissier de justice, qui pourra réaliser un constat sur internet.

Il est désormais établi que faire constater une infraction sur internet se doit de respecter un formalisme des plus stricts.

Le juge impose que la preuve d'une infraction soit établie par quelqu'un (le plus souvent un huissier de justice) qui se charge de respecter un certain nombre d'étapes lors de l'établissement de son constat.

Il devra d'abord décrire le matériel grâce auquel le constat est établi (configuration technique). Ensuite, effacer l'historique, les cookies, les répertoires de la mémoire cache de l'ordinateur avant de procéder au constat.

Puis inscrire l'adresse IP publique de la machine ayant servi à dresser le constat sur son procès-verbal dans le but, en cas de contestation, de vérifier au moyen du journal de connexion du serveur interrogé les pages réellement consultées pendant les opérations de constat. Il doit décrire le cheminement qu'il a lui-même effectué pour accéder à la page internet contenant l'infraction.

Il faut enfin matérialiser la page internet contenant l'infraction en l'imprimant puis en l'annexant au procès-verbal.

Seul le respect de cette démarche, mise en place par la jurisprudence, évitera à la preuve d'être écartée par le Tribunal. Une norme AFNOR NF Z67-147, spécifique aux constats sur internet, a d'ailleurs été publiée en septembre 2010. À titre d'exemple, la Cour d'Appel de Paris, dans un arrêt du 17 novembre 2006, a refusé d'admettre comme preuve un constat d'huissier au motif que l'huissier n'avait pas vidé les caches contenus dans la mémoire du serveur proxy avant de constater la matérialité de l'infraction de contrefaçon au cœur du litige (CA Paris, 4è ch., B. 17 nov. 2006).

Peut-on être hébergeur et éditeur en même temps ?

La réponse est oui.
A titre d'exemple, le journal « Le Monde » est **un éditeur** de service professionnel concernant les articles qui sont rédigés par ses journalistes et publiés sur le site internet, mais également **un hébergeur** des messages qui sont, cette fois, publiés sur le forum de discussion du site par des tiers ainsi que dans les commentaires situés au pied des articles (à la condition que la modération soit une modération à postériori desdits commentaires).

De façon générale, un éditeur de services professionnels sera hébergeur de tous les contenus créés par des tiers et sur lesquels il n'a aucun contrôle.

Responsabilité « éditeur / hébergeur » et politique de modération des forums de discussion et des commentaires d'articles

Compte tenu de la logique selon laquelle un éditeur peut être également hébergeur de contenus qu'il héberge sur son site à la condition qu'ils aient été créés et publiés par des tiers sans contrôle de sa part, il convient de revenir un instant sur la question de la politique de modération qui aura été mise en place par l'éditeur du site.

Si l'éditeur a mis en place un forum de discussion ou qu'il permet à ses visiteurs de commenter les articles qu'ils publient (au pied desdits articles), le statut d'hébergeur ne lui sera accordé qu'à la condition que la politique de modération soit **à posteriori et non à priori.**

La modération à posteriori implique que l'éditeur du site laisse à quiconque la possibilité de publier instantanément un contenu sans contrôle préalable de sa part alors qu'avec une modération à priori le commentaire soumis à la censure du modérateur ne sera publié qu'une fois qu'il l'aura jugé conforme à sa politique éditoriale.

Aussi paradoxal que cela puisse paraître, mieux vaut, en termes de responsabilité sur internet, mettre en place une modération à posteriori qu'une modération à priori tant sur un forum de discussion qu'à l'égard de commentaires d'articles.

En pratique, l'inconvénient d'une modération à postériori est qu'elle implique de se rendre régulièrement sur le forum afin d'éviter que ledit site se transforme en poubelle.

La modération à priori rendra l'éditeur du site directement responsable de tout ce qu'il aura accepté de publier (*alors même que le propos litigieux n'a pas été écrit par lui – il en deviendra alors l'éditeur*) alors que la modération à posteriori impliquera, pour mettre en jeu sa responsabilité directe, qu'il ait été dûment informé de l'existence dudit propos sur sa plateforme (via notification de contenus illicite, conforme à l'article 6-I-5 de la LCEN, de la part de la victime).

Comment détermine-t-on qui est l'hébergeur d'un site internet ?

Par le biais d'un who is. Il suffit d'aller sur un site du type www.whoishosting.com et de taper le nom de domaine renvoyant au site internet litigieux. Le résultat fera apparaître le nom de la société qui héberge le site internet en question.

Comment identifie-t-on l'éditeur d'un site internet qui a choisi de cacher son identité ?

Les sites illicites sont bien souvent administrés par des éditeurs qui décident sciemment de ne pas se conformer aux obligations de transparence précédemment citées (articles 6-III-1 de la LCEN).

Il devient alors compliqué de les identifier et donc de les poursuivre.
Dans ce cas, le rôle de l'hébergeur de la structure sera fondamental.
Une fois, l'hébergeur identifié par le biais d'un whois, il s'agira pour l'avocat de la personne victime du contenu qui figure sur le site de solliciter une requête présentée devant le Tribunal de grande instance territorialement compétent.

Pour des questions d'effet relatif des conventions, les informations liant un client à la société qui héberge son site web sont confidentielles et ne peuvent donc être communiquées qu'à des autorités judiciaires et/ou avec le concours d'une autorité judiciaire.

La requête présentée par l'avocat visera à ce qu'il soit autorisé, par ordonnance, à adresser à l'hébergeur une demande de communication des éléments d'identification de l'éditeur du site internet.

Ces éléments d'identification pourront être, selon les cas, (l'adresse IP, le nom, le prénom, l'email et les logs de connexion de l'éditeur indélicat).

Que peut-on faire des éléments d'identification communiqués par l'hébergeur suite à la réception de l'ordonnance transmise par l'avocat ?

Fort de ces éléments d'identification de l'éditeur (et plus spécifiquement de l'adresse IP), l'avocat sera en mesure, par le biais d'un whois spécifique aux adresses IP, de déterminer quel est le fournisseur d'accès qui correspond à l'adresse IP transmise.

Une fois le fournisseur d'accès identifié (Orange, SFR, Bouygues), il s'agira, pour l'avocat de solliciter, une nouvelle fois, le président du Tribunal de grande instance compétent, afin qu'il l'autorise à solliciter auprès du fournisseur d'accès à internet que ce dernier lève l'anonymat sur l'adresse IP qui lui aura été communiquée.

Une fois l'identité de l'internaute déterminée, il sera alors possible de poursuivre l'éditeur devant les tribunaux par la voie pénale (plainte avec constitution de partie civile ou citation directe) ou par la voie civile (assignation) en fonction de la nature de l'atteinte dont il a été à l'origine.

Différence entre l'hébergeur de la structure et l'hébergeur du contenu

Il faut bien faire la différence entre l'hébergeur d'un site internet qui est sollicité par un éditeur pour héberger la structure d'un site internet afin qu'il y apparaisse et l'hébergeur d'un contenu présent sur ledit site internet qui peut très bien être un éditeur qui héberge des articles, textes, images et vidéos publiés par un tiers sur sa plateforme (que ce soit dans les commentaires situés sous ses articles ou encore dans le forum de discussion).

L'éditeur sera alors considéré comme hébergeur des contenus illicites. C'est à lui qu'il faudra adresser la notification de contenus illicites visant à ce que ces contenus soient supprimés.

L'hébergeur de la structure du site internet (Ovh, online.net) est différent de l'hébergeur du contenu au sens où il s'agit de l'intermédiaire technique sollicité par l'éditeur pour héberger le site web dans sa globalité.

Ce dernier n'aura vocation à être contacté, en tant que fournisseurs d'hébergement, que dans l'hypothèse où le contenu illicite dont on souhaite obtenir la suppression est un élément qui a été édité (et donc créé et publié) par le responsable du site internet litigieux.

Cas pratique

Une personne édite un blog contenant des propos diffamatoires ou injurieux à l'égard de quelqu'un.
Il n'existe aucune mentions légales sur le site permettant d'identifier son éditeur.

L'avocat de la victime de l'atteinte va donc tenter de savoir de qui il s'agit. Il pourra, tout d'abord, interroger le who is du nom de domaine sur des sites internet du type « www.gandi.net » de façon à déterminer quelle est la personne qui est titulaire du nom de domaine.

Si, comme cela est souvent le cas, le titulaire a choisi l'option lui permettant de conserver son anonymat, il sera alors envisageable de demander à l'hébergeur de la structure du site, qui est celui qui a contracté un abonnement auprès de lui, des informations.

Suite à une requête auprès du président du Tribunal de grande instance compétent, un certain nombre d'éléments d'identification de l'éditeur seront alors communiqués.

Là encore, il est peu probable que les vrais noms et prénoms figurent dans le formulaire d'inscription nécessaire à la souscription d'un espace d'hébergement.

En pratique, c'est plus souvent l'adresse IP (internet protocol) qui permettra de déterminer qui est le fournisseur d'accès à qui il conviendra de demander de lever l'anonymat sur l'adresse IP qui aura été communiquée par l'hébergeur du site ou du contenu illicite.

Il arrive, en effet, que l'hébergeur sollicité pour identifier l'internaute indélicat soit l'hébergeur du contenu et non l'hébergeur du site (ex : contenu publié sur un compte Facebook).

Dans ce cas, c'est bien Facebook (éditeur de son site) mais hébergeur du contenu illicite (sur lequel il n'a aucun contrôle) qu'il conviendra de contacter.

Il sera en mesure de communiquer, suivant l'ordonnance transmise par l'avocat et signée par un juge, les logs de connexion et adresses IP de l'internaute indélicat.

Cette stratégie judiciaire visant à découvrir la véritable identité d'un internaute montre néanmoins ses limites dans l'hypothèse où celui qui cherche à cacher son identité utilise un proxy (*programme servant d'intermédiaire pour accéder à internet qui permet à son utilisateur d'obtenir une adresse IP différente de la sienne et qui pointera généralement vers un serveur étranger n'ayant aucun rapport direct ou indirect avec lu*i).

De combien de temps dispose l'hébergeur pour retirer le contenu illicite qu'on lui notifie ?

L'article 6-I-2 de la loi de juin 2004 pose que les intermédiaires techniques que sont les hébergeurs « ne peuvent voir leur responsabilité civile engagée du fait des activités ou des informations stockées » s'ils « *n'avaient pas effectivement connaissance de leur caractère illicite ou de faits et circonstances faisant apprécier ce caractère ou si, dès le moment où (ils) en ont eu cette connaissance, (ils) ont agi promptement pour retirer ces données ou en rendre l'accès impossible* ».

La loi impose donc à l'hébergeur d'agir *« promptement »* pour retirer les contenus litigieux à compter de la réception de la notification.

La question est donc de savoir dans quel délai l'hébergeur doit retirer les contenus à compter de la notification.

La Cour d'appel de Paris a considéré que le délai de 2 semaines dans lequel Google avait retiré des informations sur les services Google image[1] et Google vidéo[2] ne satisfaisait pas à l'exigence de promptitude.

Dans une autre décision du 17 février 2011, la Cour de cassation a cassé un arrêt au motif que le délai de 24h laissé par la cour d'appel à l'hébergeur pour retirer les contenus litigieux n'était pas suffisant. L'hébergeur devait en effet disposer d'un *« délai raisonnable d'analyse »* pour lui permettre de *« vérifier par lui-même le caractère manifestement illicite ou non du message incriminé »*[3].

Suite à cette décision, la Troisième chambre du TGI de Paris a jugé qu'un délai de 16 jours pour retirer des contenus était prompte, compte tenu des circonstances de fait[4].

---

[1] Paris, Pôle 5, chambre 2, 4 février 2011, Google image, JurisData : 2011-004802 : "Les retraits ne furent effectifs que plus de deux semaines après le signalement des sites litigieux, délai que les appelantes expliquent par des difficultés techniques, notamment la nécessité de traduire les signalements, mais qui ne satisfait pas à l'exigence de promptitude posée par la loi".

[2] Paris, Pôle 5, chambre 2, 9 Avril 2010, Google vidéo, JurisData : 2010-024501 : « La responsabilité de la société GOOGLE est engagée, alors qu'informée du caractère illicite de vidéos reproduisant un film documentaire mises en ligne sur le site GOOGLE Vidéo par des utilisateurs, elle a opéré le retrait de ces vidéos dans un délai supérieur à deux semaines, délai qui ne saurait être qualifié de prompt ».

[3] Civ. 1, 17 février 2011, n° 09-15857, AMEN c/ Khetah, JurisData : 2011-001675 : « Ne peut être imposée à l'hébergeur, sous couvert de « promptitude », une suspension automatique du site à réception de la notification lui faisant part du caractère prétendument illicite de son contenu, sans qu'un délai raisonnable d'analyse ne lui soit accordé pour lui permettre de vérifier par lui-même le caractère manifestement illicite ou non du message incriminé, sauf à lui imposer une mesure immédiate de censure a priori ; qu'en décidant néanmoins en l'espèce que faute d'avoir supprimé l'accès au contenu du site le jour même de la réception de la notification adressée par Monsieur X..., la société AMEN n'aurait pas agi promptement, la Cour d'appel a violé par fausse interprétation l'article 6-I-2 de la loi du 21 juin 2004 pour la confiance dans l'économie numérique. »

[4] TGI Paris, 3e ch., 4e sect., 28 avr. 2011, SPPF c/ Youtube, Google France, Google Ireland : www.legalis.net : "La société Youtube a eu connaissance des sept procès-verbaux de constat des mois de février et mars 2009, le 28 juillet 2009. Elle a effectué le retrait des fichiers en cause selon un procès-verbal de constat établi par maître Legrain, huissier de justice, les 4, 5, 6, 7, 11, 12 et 13 août 2009. Compte tenu du fait que la remise d'un procès-verbal de constat ne vaut pas notification et des difficultés matérielles rencontrées tenant à l'exploitation de ces derniers, il y a lieu d'admettre que la société Youtube a fait preuve de la promptitude requise par la loi."

La durée du « *délai raisonnable d'analyse* » dépendra donc du cas d'espèce, et notamment des contraintes techniques de l'hébergeur, de la nature de l'atteinte et du caractère manifeste ou non de celle-ci. Dans tous les cas, l'hébergeur aura largement intérêt à ne pas perdre de temps dans le traitement de la notification.

<u>Concernant la dimension internationale d'Internet</u>

Le principe veut que dès lors qu'un message est, par un service de communication au public en ligne, accessible sur le territoire national, la loi française lui est applicable et les juridictions internes sont compétentes pour en sanctionner les abus et réparer au moins les effets des dommages subis chez nous.

Elles n'ont cependant aucune exclusivité puisque, par nature, les contenus de tels services sont rendus publics dans tout autre pays. En conséquence la loi étrangère est également applicable et les juridictions sont compétentes.

En raison de la dimension internationale des réseaux de communication et donc des services de communication au public en ligne, la principale incertitude tient donc à la détermination du rattachement à un droit national, par la désignation de la loi applicable et de la juridiction compétente.

Nous verrons en la matière que les tribunaux fonctionnent bien souvent par faisceaux d'indices. Ils tiennent compte de l'endroit où se situe le siège social, du domicile du défendeur (celui que vise l'action en justice), de la langue utilisée et par extension du public visé, etc…)

Droit du commerce électronique - conflit entre noms de domaines et entre marque et nom de domaine

En matière de commerce électronique, il arrive très souvent que l'opérateur économique s'interroge sur la question de savoir quelle est la marque qu'il doit choisir et quel est le nom de domaine pour lequel il doit opter.

Parce que ces signes distinctifs ne sont pas libres d'utilisation et parce qu'ils peuvent porter atteinte aux droits de tiers et valoir à la société d'être alors poursuivie pour concurrence déloyale et ou contrefaçon, il est essentiel de savoir ce qu'est une marque, à quoi elle sert et comment on détermine le risque de confusion entre deux marques.

De la même façon, il conviendra de déterminer comment fonctionne le droit sur les noms de domaine et les questions qui peuvent se poser en la matière.

I. Le droit des marques

A. Qu'est-ce qu'une marque ?

Le Code de la propriété intellectuelle (ci-après) CPI, donne à l'article L. 711-1 une définition de la marque comme étant ***« un signe susceptible de représentation graphique servant à distinguer les produits ou services d'une personne physique ou morale »***.

Parce que le signe choisi comme marque doit être « *susceptible de représentation graphique* », cela exclu de facto les signes qui s'adressent à l'odorat ou au goût (marques olfactives ou gustatives), ainsi que les signes sonores qu'il est impossible de transcrire sur une portée musicale (rugissement, aboiement, bruit en tout genre...).

Selon la jurisprudence, s'agissant d'un signe olfactif, les exigences que doit remplir la représentation graphique ne sont satisfaites, ni par la présentation d'une formule chimique, ni par une description verbale, ni par le dépôt d'un échantillon, ni par la combinaison de ces éléments.

On distingue classiquement 3 types de marques :

1) **Marque verbale (texte)**
2) **Marque figurative (dessin – représentation graphique)**
3) **Marque semi-figurative (marque composée d'un dessin et d'un texte)**

B. Le signe visé dans la marque doit être disponible (La nécessité d'une recherche d'antériorité)

On ne peut déposer comme marque qu'un signe sur lequel n'existe aucun droit antérieur constitué au profit d'un tiers, qu'il s'agisse d'un droit antérieur limité par le principe de spécialité ou d'un droit absolu rendant le signe indisponible dans tous les secteurs de la vie économique (marque renommée).

Outre l'existence d'une marque antérieure déposée ou notoirement connue, l'antériorité peut être constituée par une dénomination sociale, une appellation d'origine ou encore un nom commercial, une enseigne et même un nom de domaine.

On ne peut adopter comme marque qu'un signe disponible, c'est-à-dire un signe sur lequel n'existe aucun droit antérieur constitué au profit d'un tiers.

L'article L. 711-4 du Code de la propriété intellectuelle donne une énumération non limitative des droits antérieurs faisant obstacle au dépôt comme marque d'un signe identique ou similaire.

« *une autre marque (CPI, art. L. 711-4, a),*

une dénomination sociale ou une raison sociale (CPI, art. L. 711-4, b), un nom commercial ou une enseigne (CPI, art. L. 711-4, c)

ou une appellation d'origine (CPI, art. L. 711-4, d) ;

quand le signe choisi comme marque a été antérieurement l'objet d'une protection par le droit d'auteur ou le droit des dessins et modèles (CPI, art. L. 711-4, e et f),

se heurte aux droits de la personnalité d'un tiers (droit au nom ou droit à l'image, CPI, art. L. 711-4, g),

ou encore aux droits d'une collectivité territoriale (CPI, art. L. 711-4, h) ».

L'article L. 711-4, a), du Code de la propriété intellectuelle permet de faire jouer une antériorité bénéficiant à une marque d'usage, c'est-à-dire une marque exploitée sans avoir été déposée, à condition qu'elle soit notoire.

C. La marque a une fonction distinctive : le principe de spécialité

Dans la classification de Nice, il existe 45 classes de produit et de services. De 1 à 34 les produits et de 35 à 45 les services.

La marque a une fonction distinctive. De cette fonction découle le principe directeur du droit des marques : le principe de spécialité. Il trouve son origine dans le principe de la liberté du commerce et de l'industrie.

Ce principe s'oppose à ce qu'un commerçant se réserve pour son usage exclusif, la propriété d'un signe dans tous les secteurs de la vie économique.

Le principe de spécialité a pour conséquence que le signe enregistré comme marque ne sera approprié par son titulaire que dans la mesure où il lui sera utile pour identifier les produits et les services qu'il aura désignés dans sa demande d'enregistrement.

Il restera donc libre pour les autres produits et une même marque, appartenant à deux propriétaires distincts, pourra identifier des produits de nature différente (par exemple Mont Blanc s'applique d'une part à des desserts, d'autre part à des stylos).

Le champ d'application de la spécialité est donc déterminé par les produits visés dans l'acte de dépôt.

Le fait qu'un dépôt se réfère à telle ou telle classe n'implique pas qu'il couvre automatiquement et nécessairement tous les produits de cette classe. Il faut tous les citer si vous souhaitez que tous les produits et services de la classe soient protégés.

D. Comment détermine-t-on qu'une marque est identique ou similaire à une autre ?

1. La nécessité d'un risque de confusion

Pour attaquer une personne pour contrefaçon de marque, pour s'opposer à l'enregistrement d'une marque ou pour annuler une marque identique ou similaire, il convient de faire préalablement la démonstration d'un risque de confusion entre votre marque et celle d'un tiers ou entre votre marque et le signe distinctif de ce tiers.

2. Définition du risque de confusion

Pour la Cour de justice (arrêt Canon du 29 septembre 1998) constitue un risque de confusion « *le fait que le public puisse croire que les produits ou services en cause proviennent de la même entreprise ou, le cas échéant, d'entreprises liées économiquement* ».

Interrogée sur ce point, la Cour de justice a jugé "*qu'un signe est identique à la marque lorsqu'il reproduit, sans modification ni ajout, tous les éléments constituant la marque ou lorsque, considéré dans son ensemble, il recèle des différences si insignifiantes qu'elles peuvent passer inaperçues aux yeux d'un consommateur moyen"* (CJCE, 20 mars 2003)

La reproduction nécessite pour démontrer le risque de confusion à la fois une similitude entre les produits (a) et entre les signes (b) désignés dans les deux marques litigieuses.

a) Similitude entre les produits

Pour apprécier la similitude entre les produits, la Cour de justice adopte une démarche objective.

La similitude entre les produits et services s'apprécie en tenant compte « *de tous les facteurs pertinents qui caractérisent le rapport entre les produits ou services (...) en particulier leur nature, leur destination, leur utilisation, ainsi que leur caractère concurrent ou complémentaire* » (arrêt Canon). Seront dès lors similaires « *des produits qui, en raison de leur nature ou de leur destination, peuvent être rattachés par la clientèle à une même origine* » (CA Paris, 28 mai 2003 : PIBD 2003, 776, III, 602).

Ont par exemple été considérés comme similaires par leur nature : des vêtements et des chaussures, parce qu'ils font partie de la catégorie générale des articles d'habillement (TGI Paris, 27 sept. 2002, Youkon : PIBD 2003, 757, III, 76).

b) **Similitude entre les signes**

Un arrêt de la CJCE SABEL c/PUMA du 11 novembre 1997 est venu préciser qu'il convient de se fonder sur l'impression d'ensemble que les marques produisent sur le consommateur, « *la similitude visuelle, auditive ou conceptuelle des marques en cause* »

Exemples de décisions de justice en la matière

Similitude visuelle (Les deux marques se ressemblent d'un point de vue visuel)

Ex : (CA Paris, 17 juin 1992, Eurostar et Eurostart : Ann. propr. ind. 1995, p. 40), (CA Paris, 18 sept. 1990, Pariscope et Pariscopie : PIBD 1991, III, 310)

Similitude phonétique (Les deux marques se ressemblent quand on les prononce malgré le fait qu'elles ne soient pas similaires visuellement)

(CA Paris, 17 mars 1981, Chairman et Sherman : Ann. propr. ind. 1981, p. 132)

Similitude intellectuelle (Les deux marques ne se ressemblent ni visuellement ni phonétiquement. Le risque de confusion est néanmoins retenu parce que le titulaire de la marque a clairement voulu évoquer dans l'esprit du consommateur un lien de rattachement entre sa marque et la première marque de façon à ce que le public puisse croire que les deux produits ou services sont commercialisés par la même entreprise).

(TGI Paris, 19 juin 1996, Le Réverbère et Le Lampadaire : PIBD 1996, III, 573).

La similitude entre les signes n'est qu'une composante du risque de confusion. Il faut démontrer également la similitude entre les produits et les services.

II. Le droit des noms de domaine

A. Qu'est-ce qu'un nom de domaine ?

Un nom de domaine (NDD en notation abrégée française ou DN pour Domain Name en anglais) est un identifiant de domaine internet. C'est l'adresse unique d'un site internet saisie par un internaute pour s'y connecter.

L'architecture d'un nom de domaine est toujours la même ; il se compose de trois parties, séparées par des points :

- un préfixe, dont la structure varie peu : "http://www" ou encore "http://", "www" signifiant "world wide web" ;

- un radical, choisi par le déposant, "yahoo", par exemple ;

- un suffixe, également appelé extension, tel ".com", ".fr" etc...

Le nom de domaine doit comporter entre 1 et 63 caractères. (exemple : **M6.fr ou T.co** (twitter)

L'extension ou le suffixe peut être un suffixe géographique de deux lettres (.fr, .pour la France, .uk pour la Grande Bretagne par exemple) ou un suffixe générique en trois lettres (.com, .net par exemple).

On distingue traditionnellement les noms de domaine ayant trait à la nationalité (domaine national de premier niveau) de ceux ayant trait à l'activité dudit site (domaine de premier niveau).

B. Qu'est-ce que le cybersquatting ?

Le cybersquatting se définit comme le fait pour une personne d'usurper le signe distinctif d'autrui en l'enregistrant en tant que nom de domaine avant, notamment, de tenter de lui revendre au prix fort.

Les signes distinctifs de l'entreprise auxquels il est fréquemment porté atteinte sont sa marque, son nom commercial, sa dénomination sociale, ou encore son enseigne.

Il peut également s'agir du nom de famille ou du nom de scène d'un individu (Zlatan Ibrahimovic, Nabila, Zahia, etc…)

1. Conflits entre noms de domaine

En cas de conflit entre deux noms de domaines enregistrés dont les signes se rapprochent ou sont identiques, c'est la date de commencement d'exploitation des noms de domaines et non la date d'enregistrement qui compte.

En clair, si vous déposez « ESGI.com » en 2002, que vous ne faites rien du nom de domaine et que l'ESGI décide en 2004 de déposer « ESGI.fr », vous ne serez pas légitimes à vous plaindre d'une exploitation illégitime par l'ESGI de votre nom de

domaine faute de l'avoir exploité en associant un site internet au nom de domaine susmentionné.

2. **Conflits entre marque et nom de domaine**

Quand il existe un conflit entre une marque et un nom de domaine enregistré postérieurement à cette marque, on estime désormais que pour qu'il y ait contrefaçon, il faut un acte consistant à utiliser un sigle identique ou similaire pour désigner des produits identiques ou similaires.

La règle de la spécialité qui existe en matière de marques est valable pour le nom de domaine.

La spécialité du nom de domaine est liée à la spécialité du site auquel il renvoie.

Il faut donc que les noms de domaines soient utilisés et pas seulement enregistrés (« réservés »), sinon le principe veut qu'ils ne soient pas des signes distinctifs, n'aient pas de spécialité et ne créent donc pas de conflits avec la marque.

Le nom de domaine, sauf exceptions, ne peut constituer un acte de contrefaçon de marque que si le nom de domaine est exploité.

Pendant longtemps, en cas de conflit entre une marque et un nom de domaine, les juges retenaient la contrefaçon selon une méthode abstraite d'identification de la spécialité du nom de domaine.

Ainsi le nom de domaine était réputé avoir pour spécialité les services de communication par réseau informatique (*service de communication en ligne ou service assimilé compris dans la classe 38 de la classification de Nice*).

Cela revenait donc à considérer que tous les noms de domaines avaient la même spécialité et cela faisait injustement tomber hors spécialité 99% des marques invoquées.

De façon paradoxale, cela ne permettait pas de reconnaître la contrefaçon alors même que les services proposés par le site auquel donnait accès le nom de domaine litigieux étaient de la même spécialité que la marque contrefaite.

Inversement, si le demandeur avait eu la présence d'esprit de déposer sa marque dans la classe 38 « service de communication en ligne », les juges retenaient d'office la contrefaçon alors que le site, auquel donnait accès le nom de domaine litigieux, exploitait, en pratique, des produits et services complètement différents.

Un important arrêt Locatour (Cass. Com. 13 décembre 2005) est intervenu pour changer la donne.

Une société possédait la marque « Locatour ».
Elle avait pour activité les voyages et le tourisme et avait déposé la marque « Locatour » pour l'activité « services de communication en ligne » (classe 38). Elle exploitait, par ailleurs, le nom de domaine locatour.fr pour donner accès à un site internet tourné vers

l'activité de tourisme.

Cette société avait décidé de poursuivre devant les tribunaux une deuxième société qui intervenait dans un domaine totalement différent. Elle avait déposé un nom de domaine locatour.com, mais ne l'utilisait pas encore.

La première société a assigné la seconde pour contrefaçon de marque (du sigle Locatour) ainsi que pour concurrence déloyale pour le dépôt de locatour.com)

La Cour d'Appel a rejeté la demande en contrefaçon concernant la marque Locatour pour l'activité de « voyages et tourisme », mais a retenu la contrefaçon pour la marque « service en ligne ».

La Cour d'Appel a déterminé que la spécialité du signe litigieux était « les services de communication en ligne », et que la non exploitation du nom de domaine ne changeait rien à cela.

La Cour de Cassation a confirmé la Cour d'Appel sur l'absence de contrefaçon pour la marque Locatour spécialité « *voyages* », mais a cassé (contredit) la Cour d'appel pour avoir retenu la contrefaçon dans la catégorie « service de communication en ligne »

Son attendu de principe est le suivant :

« *Attendu qu'un nom de domaine ne peut contrefaire par reproduction ou par imitation une marque antérieure, peu important que celle-ci soit déposée en classe 38, pour désigner des services de communication télématique, que si les produits et services offerts sur ce site sont soit identiques, soit similaires à ceux visés dans l'enregistrement de la marque et de nature à entraîner un risque de confusion dans l'esprit du public* ».

En cas de conflit entre une marque et un nom de domaine, il faut donc désormais se déterminer par rapport aux produits ou services proposés par le site auquel renvoie le nom de domaine, et non par référence automatique à la classe 38 : « service de communication en ligne ».

Dans le cas d'espèce, il aurait donc fallu que la seconde société exploite un service « classe 38 » dit de communication en ligne pour qu'il y ait véritable contrefaçon de la marque Locatour ; ce qui n'était pas le cas.

Par ailleurs, si le nom de domaine n'est pas utilisé, il faut tenir compte des services susceptibles d'être offerts compte tenu de l'activité réelle du bénéficiaire du nom de domaine.

Il faut pour cela que la société ayant réservé le nom de domaine ait une activité propre et bien délimitée similaire à celle du détenteur du nom de domaine. Ce qui en l'espèce n'était pas le cas.

Ce principe permet d'agir préventivement (mesure d'interdiction d'usage) face à une contrefaçon réelle lorsque le risque de cette dernière est important (entreprise exerce une activité analogue), même s'il est incertain.

Il y a donc des précautions à prendre quand on réserve un nom de domaine :

Sa réservation (contrairement au dépôt de la marque) n'est pas soumise à des conditions de validité et à un contrôle à priori.

Il convient donc de faire des recherches d'antériorité (rechercher s'il existe une marque, des noms commerciaux, enseignes, exploités par un concurrent avec le signe choisi comme nom de domaine).
Il faut également vérifier si les signes utilisés dans les noms de domaine sont réglementés par la loi.

L'article L.711-4 du Code de la propriété intellectuelle qui concerne les antériorités opposables aux tiers autorise l'exploitant du nom de domaine à demander l'annulation d'une marque intervenue après l'enregistrement (et l'exploitation) de son nom de domaine.

En revanche, parce que le nom de domaine n'est pas protégé au titre du droit d'auteur, il faudra passer par l'article 1382 du Code civil pour agir contre les tiers en question.

A. La question de la protection des noms de domaines génériques

A l'inverse des marques, les noms des domaines peuvent avoir ou ne pas avoir de fonction distinctive.

Une marque doit, en effet, s'abstenir de décrire strictement l'activité du produit ou service auquel elle est associée, sans quoi elle pourra être annulée. A titre d'exemple, une marque de voiture ne pourra pas s'appeler « voiture ».

Une telle exigence d'absence de caractère descriptif n'est pas imposée aux noms de domaines.

En matière de référencement, il est notamment établi que plus le nom de domaine aura un lien avec l'activité développée par le site internet et plus ce site aura des chances d'apparaître en première page de résultats de moteurs de recherche.

Ce choix pragmatique a néanmoins des implications juridiques considérables quand il s'agit, pour le titulaire de ce nom de domaine descriptif ou « générique », de poursuivre les entreprises concurrentes qui utilisent un nom de domaine similaire au sien.

La façon de gérer ce type de conflit a été tranchée par les tribunaux de façon claire depuis une célèbre affaire dite Bois Tropicaux. (*Ordonnance du TGI de Lille, 10 juillet 2001 puis Cour d'appel de Douai, 9 septembre 2003)*.

Dans cette affaire, les deux noms de domaine en cause à savoir « bois-tropicaux.com » et « boistropicaux.com » avaient été enregistrés par deux personnes morales différentes pour un même secteur d'activité. Ces noms de domaines étaient quasiment les mêmes hormis le tiret placé entre « bois » et « tropicaux ».

Après une longue procédure, la Cour d'Appel de Douai a retenu qu'il apparaissait sérieusement contestable que le fait pour le déposant second de « bois-tropicaux.com », d'avoir réservé un nom de domaine quasiment identique à la formule première réservée (cf. « boistropicaux.com »), serait-ce pour un site au contenu et aux objectifs similaires, soit constitutif d'une faute pouvant fonder une action en concurrence déloyale qui ne peut protéger contre le risque de confusion qu'en cas de signe présentant un caractère d'originalité suffisant.

Elle a précisé que ce nom de domaine était donc directement descriptif et s'apparentait à un mot-clé comme ceux utilisés pour effectuer une requête auprès d'un moteur de recherche, pour naviguer sur internet.

La Cour d'Appel a considéré que l'existence d'un trouble manifestement illicite n'a pas été jugée comme évidente et le demandeur a donc été débouté de ses demandes.

Deux affaires plus récentes ont confirmé cette position de principe.

Il s'agit d'un arrêt de la Cour d'Appel de Bastia en date du 20 mars 2013, d'une part, et du jugement du Tribunal de commerce de Paris (15ème ch) en date du 24 mai 2013, d'autre part.

Dans la première affaire, une société qui avait acquis le nom de domaine « mariagesencorse.com » avait poursuivi une personne physique au motif qu'elle exploitait le nom de domaine « mariageencorse.com ». La différence tenait donc dans l'utilisation du pluriel au mot mariage (cf. le s) dans le premier des deux noms de domaine précités.

En première instance, la demanderesse a réussi à obtenir que la défenderesse soit interdite d'utiliser le nom de domaine « mariageencorse.com » ainsi que le transfert dudit nom de domaine à son profit.

La défenderesse a, par la suite, interjeté appel de ce jugement, ce qui amené la Cour d'Appel de Bastia à infirmer le jugement entrepris.

Elle a notamment indiqué qu' : « *Il est constant qu'en vertu du principe de la libre concurrence, seul le titulaire d'un nom de domaine distinctif peut en rechercher la protection sur le fondement de l'article 1382 du code civil au titre de la concurrence déloyale, l'enregistrement d'un nom de domaine auprès d'une autorité de nommage ne lui conférant aucun droit privatif ni le bénéfice d'aucun statut juridique propre. En effet, une entreprise ne peut par le biais de son nom de domaine se voir conférer 'un droit quasi exclusif' d'exercer une activité, même sur un territoire délimité.*
Or, en l'espèce, la cour relève que le nom de domaine « www.mariagesencorse.com » est une juxtaposition d'un mot usuel et d'une provenance ou d'un lieu géographique, qui évoque l'objet et le lieu de l'activité de son titulaire sur internet »
Aussi, même s'il existe une confusion dans l'esprit des internautes, les intimés ne peuvent valablement se prévaloir de la protection du nom de leur domaine, s'agissant d'un nom de domaine générique et descriptif de l'activité de la société (…) ».

La personne physique a donc obtenu que le nom de domaine qu'elle avait dû transférer, suite au jugement de première instance, lui soit restitué.

La seconde affaire (Tribunal de commerce de Paris, 15ème chambre) en date du 24 mai 2013 opposait cette fois deux sociétés spécialisées dans les pompes funèbres. La première exploitait le nom de domaine « e-obseques.fr » tandis que la seconde exploitait un site internet à l'adresse « i-obseques-paris.fr ».

La première société a poursuivi la seconde au motif que son nom de domaine créait une confusion avec son propre site et constituait un trouble commercial qui lui était préjudiciable.

Là encore, elle a été déboutée de l'ensemble de ses demandes.

Le Tribunal de commerce a notamment retenu que : « *L'adresse internet choisie par la société Le Passage pour exercer son activité est la juxtaposition du mot obsèques et de la lettre « e-* » que « *dans « l'environnement internet, la lettre « e- »*

évoque le « e-commerce », terme désignant le commerce électronique, que « l'adresse « e-obsèques.fr » signifie « commerce électronique d'obsèques », ce qui est l'exacte activité du site internet exploité par la société Le Passage » qu'en « *choisissant des termes intégralement descriptifs, Monsieur D. Christophe et la société Le Passage s'exposaient à retrouver les mêmes termes dans des sites concurrents sur leur activité et notamment dans les réponses des moteurs de recherches qui prennent en compte la requête « obsèques » pour délivrer leurs réponses* » et enfin que « *compte tenu de leur choix, qui leur a évité les investissements indispensables pour donner une notoriété propre à une adresse internet non descriptive, Monsieur D. Christophe et la société Le Passage ne peuvent revendiquer une protection qui aboutirait à leur reconnaitre un monopole d'utilisation d'un terme descriptif* ».

Toutes ces décisions démontrent qu'en matière de noms de domaines et à l'instar de ce qui se passe en matière de marques, les termes nécessaires, génériques, usuels et descriptifs doivent absolument rester à la disposition de toutes les personnes qui exercent leur activité dans un même secteur et se concurrencent donc aucun concurrent ne peut monopoliser de tels signes et priver ainsi les autres de leur libre usage dans leur profession.

D'un point de vue plus pratique, il est donc nécessaire que la société qui décide d'enregistrer un nom de domaine veille à ne pas en choisir un trop générique (et donc descriptif de son activité), sauf à accepter d'emblée l'idée qu'elle puisse être copiée par une autre société concurrente à laquelle il lui sera difficile de reprocher quoi que ce soit.

B. La résolution judiciaire ou arbitrale des conflits en matière de noms de domaine

Le cybersquatting peut être combattu tant par la voie judiciaire que par celle de l'arbitrage (procédure extrajudiciaire de règlement des litiges).

Afin d'obtenir le transfert effectif d'un nom de domaine, la victime devra engager une action au fond devant les tribunaux ou alors utiliser une procédure alternative de règlement des litiges. Cette dernière présentera alors l'avantage d'aboutir dans un délai qui excède rarement les quatre mois suivant la saisine.

L' inconvénient principal de ces procédures alternatives, connues notamment sous l'acronyme UDRP pour les noms de domaine en .com, .org et .net ou SYRELI pour ceux en .fr, est qu'elles ne possèdent aucun caractère dissuasif.

Même si un transfert du nom de domaine litigieux est ordonné, la décision ne pourra être accompagnée ni de dommages-intérêts ni même d'un remboursement des frais de procédure engagés par le demandeur, à la charge du cybersquatteur.

Ce type de condamnations reste, en effet, l'apanage des décisions de justice prononcées à la suite d'actions engagées devant les tribunaux.

Par ailleurs, cette procédure alternative de règlement des litiges n'est possible qu'à la condition que le requérant (celui qui est à l'origine de la demande) ait déposé une marque avant la date d'enregistrement du nom de domaine litigieux.

Il conviendra donc, outre de cette condition sine qua non, pour l'entreprise de bien peser le pour et le contre avant de décider de la stratégie à adopter pour faire cesser un trouble lié à la reprise par un cybersquatteur de son signe distinctif dans un nom de domaine.

Droit du commerce électronique et cybersurveillance du salarié sur son lieu de travail

La protection de la vie privée du salarié sera atténuée sur son lieu de travail, mais le respect de sa vie privée continuera à exister.

Le caractère professionnel fait, en effet, disparaître certains éléments de protection, mais en aucun cas l'ensemble.

Les mesures de restrictions de la liberté d'expression mises en place par l'employeur devront être proportionnées au but poursuivi et fondées sur des motifs pertinents et suffisants.

Un arrêt du 6 décembre 1992 a souligné que le droit au respect de la vie privée n'a aucune raison de principe de ne pas s'appliquer aux activités professionnelles ou commerciales.

C'est aux juridictions (cf. tribunaux) qu'il appartiendra de contrôler, à postériori, les éventuelles atteintes aux droits qui découleront de ce qu'aura mis en place le salarié.

Une interdiction absolue d'usage non professionnel des ordinateurs et des réseaux serait irréaliste et le plus souvent inopportune, en tout cas inconciliable avec l'évolution des comportements.

Dans ce domaine, l'arrêt dit Nikon du 2 octobre 2001 s'avère être un arrêt fondateur par rapport à cette problématique : il pose les fondements des restrictions au pouvoir de l'employeur.

> « *Le salarié a droit même au temps et au lieu de travail au respect de sa vie privée, celle-ci implique en particulier le secret des correspondances. L'employeur ne peut dès lors, sans violation de cette liberté fondamentale, prendre connaissance des messages personnels émis par le salarié et reçu par lui grâce à un outil informatique mis à sa disposition pour son travail, et ceci même au cas où l'employeur aurait interdit une utilisation non professionnelle de l'ordinateur* ».

A. La question du contrôle des mails et des documents créés par le salarié

L'envoi d'un message électronique par une personne à une autre personne, constitue, par principe, une communication privée.

La démarche consistant pour l'employeur à effectuer des manœuvres nécessaires pour pénétrer dans la messagerie privée de son salarié caractérise donc le détournement de correspondance visé par le Code pénal.

Concernant la messagerie professionnelle du salarié, tout dépendra du nom sous lequel le fichier a été enregistré.

En règle générale, lorsqu'un salarié crée un fichier à partir de l'ordinateur mis à sa disposition par l'employeur pour les besoins de son travail, ledit fichier est présumé avoir un caractère professionnel. Cela signifie que l'employeur est en droit de l'ouvrir et de le consulter hors la présence du salarié.

Cette prérogative résulte du pouvoir de direction de l'employeur qui est en droit de consulter l'activité de ses salariés pendant leur temps de travail.

1. <u>Quelles sont les conditions d'accès aux fichiers personnels du salarié ?</u>

Le respect de la vie privée du salarié implique que certains fichiers stockés sur l'ordinateur ne peuvent être librement consultés par l'employeur.

C'est le cas des fichiers ou des e-mails signalés comme étant « personnels et privés ». (Cass, soc, 2 octobre 2001 dit arrêt Nikon).

L'important est que le nom du fichier choisi par le salarié ne laisse planer aucun doute sur le caractère « privé » du document.

Dans cette hypothèse, celle où le caractère privé du mail ou du document ressort de son objet ou de son titre, l'employeur pourra, par exception, y accéder pour 3 raisons :

a) **en cas de risque ou d'événement particulier (**pour l'entreprise)

b) **en présence du salarié,**

c) **ou lorsque ce dernier a été « dument appelé », c'est-à-dire convoqué en vue de l'ouverture du fichier mais qu'il n'est pas venu.**

Les tribunaux sont très stricts concernant l'appellation des fichiers que le salarié veut protéger du regard de l'employeur.

En effet, dans un arrêt du 10 mai 2012 (Cass, soc, 10 mai 2012), la Cour de cassation a jugé que l'intitulé « mes documents » ne conférait pas un caractère personnel au fichier stocké sur l'ordinateur professionnel du salarié, de sorte que l'employeur avait le droit de le consulter. De la même manière, un dossier comportant comme titre les initiales du salarié « JM », ou son prénom « Alain », n'ont pas été considérés comme suffisants pour donner au fichier un caractère privé.

Plus récemment, dans une affaire où un salarié avait pensé pouvoir interdire l'intégralité de l'accès de son disque dur à l'employeur en renommant le disque « D : / données personnelles », la cour de cassation a jugé qu'une telle dénomination ne pouvait conférer un caractère personnel à la totalité des données contenues sur le disque dur (Cass, soc, 4 juillet 2012). En conséquence, si un salarié est autorisé à stocker des dossiers « personnels » sur son disque dur, ce dernier ne peut s'arroger l'exclusivité de l'accès au disque dur au motif de l'avoir renommé « données personnelles ».

B. Réglementation spécifique aux moyens de contrôle de l'activité internet du salarié

En vertu de son pouvoir de direction, l'employeur peut décider de limiter l'utilisation d'internet et notamment des réseaux sociaux à partir des outils informatiques mis à la disposition du salarié par l'entreprise à la condition que cette limitation soit proportionnée au but recherché.

Par exemple, dans certains cas, des restrictions voire une interdiction d'utiliser des réseaux sociaux pourront être décidées par l'entreprise pour des raisons de sécurité.

L'employeur a également le droit, pour autant que les instances représentatives du personnel aient été informées et consultées sur l'existence et la mise en œuvre des dispositifs de contrôle, de contrôler l'activité de ses salariés pendant leur temps de travail.

Ce contrôle pourra avoir pour objet de déceler d'éventuels comportements fautifs ou illicites des salariés qui pourraient avoir pour conséquence d'engager la responsabilité de l'entreprise.

<u>Il faut néanmoins que l'employeur :</u>

1. prenne des mesures proportionnées au but recherché du point de vue des droits des personnes et des libertés individuelles (article L. 1121-1 du Code du travail);

2. informe et consulte le comité d'entreprise, préalablement à la décision de mise en œuvre dans l'entreprise, sur les moyens ou les techniques permettant un contrôle de l'activité des salariés (article L. 2323-32 du Code du travail) Le Comité d'entreprise doit être consulté sur les mutations technologiques, et doit être informé, préalablement à l'introduction dans l'entreprise de traitements automatisés de gestion du personnel, mais aussi à la mise en œuvre dans l'entreprise de moyens ou de techniques permettant un contrôle de l'activité des salariés.

3. informe préalablement les salariés de l'existence, des modalités, de la finalité du dispositif de contrôle, de la durée de conservation ou de sauvegarde des données de connexion et des conséquences éventuelles (par exemple, sanctions disciplinaires).
   Cela résulte des dispositions prévues par l'article L. 1222-4 du Code du travail et par la loi relative aux fichiers, à l'informatique et aux libertés du 6 janvier 1978 modifiée;

4. réalise les formalités préalables nécessaires au titre de la loi du 6 janvier 1978 relative aux fichiers, à l'informatique et aux libertés modifiée (déclaration normale ou simplifiée des fichiers constitués à l'aide de l'outils de contrôle)

<u>Application pratique de ces différentes règles en matière de cybersurveillance des salariés</u>

En cas de non-respect des règles énoncées précédemment, la preuve obtenue par le dispositif de contrôle ne pourra pas être utilisée en cas de litige avec le salarié sauf en matière pénale. Il sera impossible de licencier valablement un salarié pour une raison obtenue grâce à l'un des moyens techniques ne respectant pas les règles précitées. Le licenciement éventuel pourra être considéré comme étant sans cause réelle et sérieuse.

À noter, par ailleurs, que l'entreprise ne pourra pas contrôler les équipements personnels des salariés.

Désormais le droit social a intégré les enjeux de l'utilisation de l'outil internet au sein de l'entreprise.

La CNIL admet que l'entreprise mette en place des dispositifs de filtrages de l'accès à certains sites Internet via le réseau de l'entreprise, y compris par des pare-feux.

Cela peut permettre de régler par anticipation un certain nombre de difficultés.
Il faut cependant respecter les procédures de déclaration à la CNIL.

Un arrêt de la chambre sociale de la Cour de cassation en date du 6 mars 2007 a eu l'occasion d'établir que l'utilisation par un salarié de l'accès à internet de l'entreprise, à des fins non professionnelles, pour visiter des sites prohibés constitue une cause réelle et sérieuse de licenciement.

L'employeur est autorisé, compte tenu du fait que les connexions à internet du salarié sont présumées avoir un caractère professionnel, à rechercher celles-ci de façon à les identifier et ce, que le salarié soit ou non présent.

Un salarié a vu, le 21 septembre 2011, la Cour de cassation confirmer son licenciement pour faute grave au motif qu'il avait utilisé un logiciel de suppression des fichiers temporaires et autres cookies de son ordinateur professionnel afin de cacher à son employeur le fait qu'il naviguait sur une multitude de sites « d'activités sexuelles et de rencontres ».

La possibilité qui est offerte à l'employeur de contrôler les connexions de ses salariés peut ainsi l'amener à sanctionner légitimement l'usage abusif d'internet, à des fins non professionnelles, qu'il soit caractérisé par sa durée ou par son objet.

Rappelons qu'il faudra toutefois que l'employeur ait pris le soin d'informer et consulter les représentants du personnel des moyens de contrôle qu'il entend mettre en place, qu'il en ait informé les salariés individuellement et qu'il ait procédé aux formalités de déclarations adéquates auprès de la CNIL.

C. La mise en place d'une charte informatique

La charte informatique va pouvoir préciser les conditions dans lesquelles l'employeur va pouvoir réclamer l'accès aux données.

La charte renforcera la légitimité de l'intervention de l'employeur et la force des contraintes susceptibles d'être imposées au salarié.
D'ou la nécessité de développer des chartes informatiques dans les entreprises.

Par ailleurs la jurisprudence a établi que le non respect de la charte informatique peut être constitutif d'une faute grave justifiant le licenciement et rendant impossible le maintien du salarié pendant la durée du préavis.

Ces chartes ne sont pas obligatoires au sein d'une entreprise.

Aucun texte n'impose l'adoption dans l'entreprise de règles d'utilisation des technologies de l'information et de communication.

La charte constitue néanmoins un instrument efficace de sécurisation de l'entreprise, de prévention, de sensibilisation et de responsabilisation des salariés. Les entreprises s'engagent de plus en plus régulièrement dans des démarches de ce type. Cependant, la mise en place d'une charte implique une mobilisation et la conduite collective de travaux au sein de l'entreprise (rédaction, adoption, évolutions du contenu...).

L'absence d'une charte n'empêchera pas l'entreprise de prendre des mesures, à la suite d'un comportement fautif ou illicite du salarié, fondées sur la mauvaise exécution du contrat de travail ou encore sur le droit civil ou pénal par exemple.

<u>Une charte d'entreprise sur l'utilisation d'internet permettra :</u>

- d'inciter la conduite en interne de réflexions et d'impliquer les salariés sur l'utilisation de l'outil qu'est internet

- d'informer et de sensibiliser les salariés sur :

  - certaines conséquences liées à l'utilisation des réseaux sociaux : (échange d'informations confidentielles, risques liés à la sécurité informatique...)

  - la politique de communication de l'entreprise sur les réseaux sociaux ;

  - les éventuels moyens mis en place pour contrôler l'utilisation par les salariés d'internet *via* les moyens informatiques fournis par l'entreprise.

- de protéger l'entreprise contre la mise en cause de sa responsabilité juridique.

Dans la pratique, la valeur juridique de la charte dépendra de la force obligatoire que l'entreprise souhaitera lui donner en fonction du degré de sensibilité interne du sujet.

Les documents ou « chartes » intégrés ou annexés au règlement intérieur ainsi que les règles incluses directement dans le contrat de travail du salarié ont une valeur contraignante pour les salariés.

Les autres documents ou « chartes » n'auront qu'une valeur informative ou pédagogique.

Dès lors, différentes situations pourront être distinguées :

- **Si la charte n'est pas intégrée au règlement intérieur** mais qu'elle constitue un document autonome, elle aura alors une valeur informative et de sensibilisation des salariés.

Cela implique que le non-respect des éventuelles obligations y figurant par le salarié ne pourra pas faire spécifiquement l'objet des sanctions disciplinaires prévues par le règlement intérieur.

L'entreprise pourra, en revanche, s'appuyer, en cas de problème, sur les obligations découlant du contrat de travail (obligation de loyauté...) ou encore sur les règles générales du droit.

- **Si la charte est intégrée au règlement intérieur de l'entreprise (dans le texte ou en annexe),** Il conviendra alors de respecter le formalisme prévu par le Code du travail, et notamment son article L. 1321-4, en matière d'adoption et de modification du règlement intérieur à savoir :

- soumettre à l'avis du Comité d'entreprise ou à défaut des délégués du personnel, et, pour les matières relevant de l'hygiène et de la sécurité des travailleurs, à l'avis du comité d'hygiène, de sécurité et des conditions de travail ;

- transmettre le document à l'inspecteur du travail et prendre en compte ses observations le cas échéant ;

- accomplir des formalités de dépôt et de publicité au greffe du Conseil de prud'hommes.

Dans ces conditions, le non-respect des obligations prévues dans la charte pourra exposer le salarié aux sanctions disciplinaires prévues par le règlement intérieur.

Si ce formalisme n'est pas respecté, le règlement intérieur (et par conséquent les règles d'utilisation d'internet et des réseaux sociaux au sein de l'entreprise) n'aura pas de caractère contraignant pour le salarié.

Droit du commerce électronique et droit d'auteur

Le droit de la propriété intellectuelle est source d'importants conflits dans le commerce électronique, qu'il s'agisse de contrefaçon ou de concurrence déloyale liés à la marque, au nom de domaine ou encore à l'image.

A ses débuts, le droit de la propriété intellectuelle correspondait à 80% du contentieux en matière de commerce électronique. Il est moins important mais, reste assez conséquent.

Histoire du droit de la propriété intellectuelle

Le droit de la propriété intellectuelle a été codifié en 1992 en droit français, mais il s'agit d'un droit protégé en France depuis 1791 et 1793.

Le droit d'auteur se définit comme le droit qu'ont les auteurs sur leurs œuvres littéraires et artistiques dès leur création.
Les droits voisins du droit d'auteur se définissent comme ceux qui confèrent un monopole d'exploitation sur un bien incorporel accordé aux auxiliaires de la création littéraire et artistique.

Le droit d'auteur comprend notamment le droit de la propriété littéraire et artistique et le droit de la propriété industrielle.

Le droit de la propriété littéraire et artistique se distingue notamment du droit de la propriété industrielle (marques, brevet, dessins et modèles) par le fait qu'il n'exige pas de dépôt pour faire naître un droit (article L. 111-1 du Code de la propriété intellectuelle alors qu'à l'inverse le droit ne naîtra en matière de propriété industrielle que suite à un acte juridique que constitue le dépôt.

A côté du droit d'auteur, il existe ce que l'on appelle les droits voisins du droit d'auteur.

Ces droit voisins concernent, d'une part, les droits des artistes interprètes relatifs à ceux qui exécutent des œuvres littéraires et artistiques (chanteurs) et, d'autre part, le droit des producteurs de phonogrammes et de vidéogrammes qui sont ceux des producteurs de disques et de vidéos.

Les droits voisins sont droits détenus par leurs titulaires pendant 50 ans après la première fixation sur un support de l'œuvre ou 50 ans après sa première divulgation.

Qu'entend-t-on par droit d'auteur ?

Le droit d'auteur est conditionné par un critère d'originalité. Un droit d'auteur se définit comme une création intellectuelle qui a une forme d'expression remplissant la condition d'originalité, c'est-à-dire remplissant l'empreinte de la personnalité de l'auteur.

Cela peut-être une création musicale, littéraire. Il n'y a pas besoin d'un support physique, il faut seulement que ça soit exprimé (dans un discours par exemple).

Contrairement à une croyance erronée, le droit d'auteur n'a nul besoin d'être déposé ou enregistré pour être protégé (à l'inverse de la marque du dessin et modèle ou encore du brevet).

Aucune formalité n'est donc exigée pour bénéficier de la protection reconnue par le droit d'auteur : l'œuvre est protégée du seul fait de sa création. Nul besoin d'un dépôt, ni même d'apposition de la mention « copyright » ou « tous droits réservés » puisque, comme nous avons pu le voir, le droit d'auteur s'acquiert automatiquement dès que le l'œuvre est créée, sans autre formalité.

<u>Le dépôt est un un simple moyen de preuve de l'antériorité</u>

La mention copyright ou (©) suivie de l'année de première publication n'est donc pas nécessaire pour l'acquisition des droits d'auteur, mais elle est utile pour signaler aux tiers la date de création et informer ce dernier du fait qu'il entend se prévaloir de ses droits.

L'auteur peut également choisir de déposer son œuvre chez un notaire, un huissier, sur un site de dépôt électronique (par horodatage), auprès d'une société de gestion collective ou encore s'envoyer à lui-même ou à un tiers l'œuvre sous pli fermé avec accusé de réception l'œuvre en question sans ouvrir l'enveloppe lors de la réception, le cachet de la poste faisant foi.

L'article L. 111-1 du Code de la propriété intellectuelle dispose que : *« L'auteur d'une œuvre de l'esprit jouit sur cette œuvre, du seul fait de sa création, d'un droit de propriété incorporelle exclusif et opposable à tous* ».

Les juges acceptent très facilement la condition d'originalité dès qu'il ne s'agit pas de la reproduction à l'identique de ce qui a été fait.

Ils ne tiennent pas compte du mérite pour apprécier le fait que le critère d'originalité existe. Toute œuvre qui remplit la condition d'originalité est par essence protégeable au titre du droit d'auteur.

La jurisprudence peut néanmoins considérer que la reproduction manuelle d'une création antérieure est une œuvre originale pour peu qu'elle porte la marque de son auteur.
Pour autant, il faudra respecter aussi les droits sur l'œuvre antérieure. Ce sera le cas d'une adaptation cinématographique d'un livre, de samples musicaux.
Il n'est pas possible de prétendre avoir respecté les droits d'auteur sans avoir obtenu l'autorisation des auteurs de l'œuvre d'origine. Vous pouvez être poursuivi pour contrefaçon pour ne pas l'avoir fait.

Le propriétaire des droits est traditionnellement celui qui l'a créée, mais il peut y avoir des œuvres que l'on appelle des œuvres de collaboration où plusieurs personnes sont co-auteurs ou encore des œuvres collectives comme celle « *créée sur l'initiative d'une personne physique ou morale qui l'édite, la publie et la divulgue sous sa direction et son nom et dans laquelle la contribution personnelle des divers auteurs participant à son élaboration se fond dans l'ensemble en vue duquel elle est conçue, sans qu'il soit*

possible d'attribuer à chacun d'eux un droit distinct sur l'ensemble réalisé ».

Les prérogatives du titulaire d'un droit d'auteur

L'auteur bénéficie d'un droit patrimonial (1) et d'un droit moral (2)

1 - Le droit patrimonial

Il bénéfice d'un droit patrimonial qui s'entend d'un monopole d'exploitation de l'œuvre.

Il s'agit d'un **droit de reproduction** consistant au fait de contrôler toute fixation matérielle de l'œuvre.

Il possède également **un droit de représentation** qui consiste en un droit pour l'auteur de contrôler toute communication au public de l'œuvre.

L'auteur peut donc contrôler la représentation de son œuvre au cinéma, au théâtre, dans un concert, sur Internet, à la télévision.

L'auteur peut cependant procéder à la transmission des droits patrimoniaux. Cette transmission est conditionnée par l'article L.131-3 du CPI.
L'acte de cession des droits patrimoniaux doit être très précisément détaillé. Si celui n'est pas assez précis, alors on considère qu'aucune autorisation n'a été donnée (et dans ce cas là, la personne qui exploite devient contrefacteur)

L'auteur bénéficie également d'un **droit de suite** (droit de toucher un pourcentage sur la revente de l'œuvre.

La durée des droits patrimoniaux s'étend jusqu'à 70 ans après la mort de l'auteur ou du dernier des auteurs. Différent des droits voisins qui durent 50 ans et qui bénéficient aux auxiliaires de la création.

Passé ces délais, l'œuvre tombe dans le domaine public et tout le monde peut l'utiliser ; à la condition de respecter les droits moraux.

2 - Le droit moral

Le droit moral est un droit qui a pour objet de protéger la personnalité de l'auteur telle qu'elle s'est exprimée dans l'œuvre. Sa durée est perpétuelle.

Il comprend le **droit de divulgation** (seul l'auteur peut donner son accord pour que l'œuvre fasse l'objet d'une première divulgation), **le droit au respect de l'œuvre** (Il faut respecter l'œuvre pour respecter la personnalité de l'œuvre), **le droit au respect de l'intégrité de l'œuvre** (droit au respect de l'esprit de l'œuvre, droit de contrôler le contexte dans lequel est utilisée l'œuvre (dans un œuvre érotique, dans une publicité), **le droit à la paternité de l'œuvre** (droit à ce que le nom de l'auteur soit affiché lors de l'exploitation de son œuvre même s'il est possible d'y renoncer (ex : utilisation d'un nègre littéraire), le **droit de retrait ou de repentir** (Droit de l'auteur de revenir sur un contrat par lequel il s'est engagé à accorder une exploitation, avant ou après le début de l'exploitation, moyennant une indemnisation suffisante du cocontractant).

Droit du commerce électronique, droit de l'informatique et droit d'auteur

On a souvent voulu présenter internet comme un moyen d'accès immatériel et planétaire aux œuvres dans lequel le droit d'auteur n'avait pas à s'appliquer. Ce raisonnement a été tenu surtout par des non juristes.

D'autres arguments ont été avancés pour soutenir que le droit d'auteur serait applicable par principe sur le réseau mais serait inadapté car dépourvu d'efficacité : impossibilité d'identifier les auteurs, d'engager des poursuites en raison de la dimension du réseau. Le droit d'auteur serait, de facto, inapplicable en pratique à internet.

On peut toujours opposer également en opportunité que le droit d'auteur se justifie aussi par l'idée qu'il permet à l'auteur d'être rémunéré, de vivre de l'exploitation et d'être en situation de créer une nouvelle oeuvre. S'il n'était pas protégé, l'auteur pourrait créer moins. Cela pourrait limiter le nombre d'œuvres nouvelles.

C'est effectivement ce qu'il s'est passé, la révolution technique du réseau ne s'est accompagné d'aucune révolution juridique. Les situations ont été réglées par applications des règles de droit d'auteur, règles suffisamment générales pour s'appliquer.

Il y a eu parfois des difficultés de qualifications, aujourd'hui surmontées. Même le Peer to Peer est pris en compte pas le droit d'auteur, même les techniques les plus récentes relèvent de règles classiques du droit d'auteur.

Pour l'essentiel, ce sont les concepts de base qui ont été mis en œuvre, qui ont trouvé à s'appliquer.

L'article L.122-1 du code de la propriété intellectuelle énonce le contenu du monopole d'exploitation (droit de reproduction et de représentation).

L'article L.122-4 précise « *Toute représentation ou reproduction intégrale ou partielle faite sans le consentement de l'auteur ou de ses ayants droit ou ayants cause est illicite. Il en est de même pour la traduction, l'adaptation ou la transformation, l'arrangement ou la reproduction par un art ou un procédé quelconque* ».

Cet arsenal conçu en termes généraux permet de sanctionner les exploitations illicites d'œuvres sur le réseau.

Le droit de reproduction sur internet

L'article L.122-3 du Code de la propriété intellectuelle dispose que la reproduction consiste en la fixation matérielle de l'œuvre par toute procédé qui permette de la communiquer au public de manière indirecte.

La formulation de cet article laisse apparaître l'indifférence du changement de support. On distingue l'œuvre de son support matériel. L'auteur qui cède le support matériel ne cède aucun droit d'auteur.

On ne tiendra également pas compte du caractère permanant ou provisoire de la reproduction. Il s'agira de toute fixation matérielle même provisoire, un dessin sur le sable, une sculpture dans la glace, une apparition sur un site quelques heures sont des reproductions.

Indifférence aussi du caractère partiel ou non de la reproduction.

Il faut néanmoins que les caractéristiques originales de l'œuvre soient reproduites.

La question s'est déjà posée à propos des manipulations des œuvres musicales - sampling musicaux (traitement des données d'une œuvre pour créer un nouveau morceau).
Si on retrouve les caractéristiques originales d'une œuvre, on est tributaire de l'œuvre. Il faut retrouver une ou des caractéristiques de l'œuvre originale dans l'œuvre seconde. Le juge pourra recourir à l'expertise afin de déterminer si une ou des caractéristiques de l'œuvre se retrouve. On ne se réfère pas à l'utilisateur moyen.

L'application de ces règles aux actes accomplis sur internet

La 1ère décision en ce sens remonte au 14 août 1996. Par deux ordonnances de référé du TGI dans deux affaires dites Brel et Sardou.

Des étudiants de grandes écoles scientifiques avaient mis en ligne sur leur page personnelle des textes et des extraits musicaux de deux artistes, les titulaires des droits ont agi en justice après avoir fait constaté cela par l'Agence de Protection des Programmes. Les sites en cause étaient accessibles à tout utilisateur du réseau. Les titulaires ont saisi le juge des référés (juge de l'urgence) pour mettre fin à l'exploitation de l'œuvre. Ils prétendaient que le stockage numérique des œuvres sur les pages constituait des actes de reproduction et ont obtenu gain de cause.

Dans une affaire TGI, (ordonnance de référé) 5 mai 1997, affaire Queneau, un personne avait numérisé et installé sur son site une œuvre de Raymond Queneau « mille milliard de poèmes », sans l'autorisation du titulaire des droits et le tribunal a estimé que cette opération constituait une reproduction de l'œuvre qui requiert en tant que telle l'autorisation préalable de l'auteur. Une numérisation sans autorisation est donc illicite et constitue donc une contrefaçon.

Dans une Ordonnance de référé du 3 février 1998 du TGI Strasbourg, il s'agissait cette fois d'un conflit entre journalistes et éditeurs de presse dans une affaire sur les dernières nouvelles d'Alsace. La diffusion d'articles du journal papier sur la version web du journal qui n'avait pas été préalablement autorisée par les journalistes a été condamnée comme relevant d'une contrefaçon. Le juge a indiqué que la diffusion sur Internet de l'article est bien un nouveau mode de reproduction soumis à autorisation.

La question a donc été réglée par des conventions collectives, qui prévoient désormais des rémunérations supplémentaires pour les salariés, y compris pour les hypothèses ou le journal serait ré-exploité dans son ensemble sur internet.

Les exceptions au droit d'auteur

La loi sur le droit d'auteur comporte des exceptions prévues à l'article L.122-5 qui s'appliquent aussi bien au monde physique qu'à internet.

Le Traité de l'OMPI indique, en effet, que les exceptions traditionnelles ont vocation à s'appliquer aux réseaux. Il convient d'examiner les exceptions traditionnelles ainsi que les exceptions nouvelles issues de la loi du 1er août 2006 (loi DADVSI)

Toutes les exceptions au droit d'auteur sont énumérées à l'article L.122-5 CPI.

1) Exception de copie privée

L'article L. 122-5 al. 1 du CPI prévoit que lorsque l'œuvre a été divulguée, l'auteur ne peut interdire « *les copies ou reproduction strictement destiné à l'usage du copiste et non destiné à un usage collectif* ».

S'agissant des logiciels et des bases de données numériques, il n'existe pas de droit à la copie privée, mais un droit à une copie de sauvegarde.

La reproduction d'une oeuvre sur un site ne relève pas de l'exception de copie privée.

Les ordonnances de référé précitées dites Brel & Sardou ont retenu que la reproduction sur un site Internet d'une œuvre ne relève pas de la copie privée malgré l'argumentaire des défendeurs qui indiquaient n'avoir aucune volonté de communiquer au public les œuvres et qu'il s'agissait d'un simple usage personnel.

L'argumentation a été rejetée car des tiers pouvaient accéder à leur site privé.
On doit considérer qu'offrir les moyens à des tiers de faire des reproductions exclu de fait l'exception de copie privée.
Logique car dans ce cas là l'usage n'était pas strictement réservé à l'usager et à ses proches.

2) Exception de parodie

La parodie, le pastiche ou la caricature sont des exceptions au droit d'auteur, c'est-à-dire des exceptions, pour l'auteur de l'œuvre parodiée, à son droit d'autoriser ou d'interdire. Il ne pourra pas s'y opposer. En général, on parle de pastiche en matière littéraire, la parodie étant utilisée dans le domaine musical et la caricature dans le domaine des arts graphiques. Mais chacune de ces notions recouvrent bien la même chose : l'article L122-5 du Code de la propriété intellectuelle dit bien que « lorsque l'œuvre a été divulguée, l'auteur ne peut interdire la parodie, le pastiche et la caricature, compte tenu des lois du genre ».

La loi du genre signifie que c'est la jurisprudence (c'est-à-dire les décisions de justice dans des affaires portées devant les tribunaux) qui va fixer les critères qui permettront d'appliquer ou non l'exception.

La Cour d'Appel de Paris s'est prononcée sur un cas intéressant le 18 février dernier. L'affaire concernait une collection intitulée « Les aventures de Saint Tin et de son ami Lou ».

Tout le monde a bien sûr reconnu dans ce titre l'Œuvre d'Hergé (Tintin).

La société Moulinsart, qui gère les droits sur les œuvres d'Hergé, avait attaqué la collection de Gordon Zola, du nom de l'auteur de la série, ainsi que son éditeur, le Léopard Masqué, pour contrefaçon des œuvres d'Hergé. Or, la Cour d'Appel a relevé une dimension parodique évidente, qui peut être d'emblée perçue à la lecture du titre et à la vue des couvertures, tous deux renseignant le lecteur sur la volonté des auteurs de faire rire. Les critères sont retenus : nous étions bien dans le pastiche.

Attention donc à bien rentrer dans cette définition du pastiche si l'on veut éviter la requalification en contrefaçon, ou en agissements parasitaires.

Ex : Publicité de la marque Renault parodiant une publicité de la marque Opel.

3) L'exception de courte citation

Selon l'article L.122-5 du CPI, il faut répondre à 3 critères pour pouvoir bénéficier de l'exception de courte citation :

Une citation courte :

Elle s'évaluera par rapport aux dimensions de l'œuvre citée, mais aussi de l'œuvre citante.

La citation doit être justifiée par certaines finalités (critique, polémique, pédagogique scientifique ou d'information) de l'œuvre d'origine.

La citation doit être intégrée à une œuvre ayant une autonomie en dehors des citations).

Dans l'affaire Queneau (référé TGI Paris), le défendeur invoquait l'exception de copie privée et aussi l'exception de courte citation. Inopposable puisque l'œuvre était intégralement reproduite par petits morceaux.

Traditionnellement, on rejette cette exception pour les œuvres graphiques ou plastiques, car soit l'œuvre est intégralement reproduite, soit on porte atteinte à l'intégrité de l'œuvre (droit moral).

La loi a néanmoins intégré une exception légale pour les commissaires priseurs en 1997 puis en 2000 pour les ventes judiciaires.

4) L'exception d'information

Elle est prévue à l'article L.122-5 9° du CPI.

« La reproduction ou la représentation, intégrale ou partielle, d'une œuvre d'art

graphique, plastique ou architecturale, par voie de presse écrite, audiovisuelle ou en ligne, dans un but exclusif d'information immédiate et en relation directe avec cette dernière, sous réserve d'indiquer clairement le nom de l'auteur » est permise.

Cette exception vise à combattre la jurisprudence Utrillo : exposition sur Utrillo, qui avait fait l'objet d'un reportage.
La jurisprudence française a rejeté cette possibilité d'informer et condamné le défendeur pour contrefaçon.

L'alinéa 2 de l'article L. 122-5 9° précise que « Le premier alinéa du présent 9° ne s'applique pas aux œuvres, notamment photographiques ou d'illustration, qui visent elles-mêmes à rendre compte de l'information »

Cela sert à empêcher qu'une photo de presse, qui est en soit une œuvre, puisse être librement exploité par un tiers en prétendant bénéficier de l'exception d'information.

5) L'exception de revue de presse

Elle est possible à la condition qu'elle soit élaborée par un organe de presse (qui ne saurait s'opposer à l'utilisation réciproque de ses propres articles), que le regroupement soit organisé par thème ou événement et que la revue de presse respecte le droit moral et patrimonial des auteurs (citations courtes qui ne doivent pas dispenser le lecteur de lire l'article original, mention complète de l'auteur et de l'organe source permettant au lecteur de s'y reporter aisément).

6) Exception à des fins de conservation par des bibliothèques

L.122-5 8° du CPI.

« La reproduction d'une œuvre et sa représentation effectuées à des fins de conservation ou destinées à préserver les conditions de sa consultation à des fins de recherche ou d'études privées par des particuliers, dans les locaux de l'établissement et sur des terminaux dédiés par des bibliothèques accessibles au public, par des musées ou par des services d'archives, sous réserve que ceux-ci ne recherchent aucun avantage économique ou commercial » est permise.

7) Exception à des fins d'enseignement et de recherche

8) Exception en faveur des reproductions provisoires

L.122-5 6° du CPI.

Il autorise les fixations matérielles provisoires lorsqu'elles sont effectuées par des prestataires techniques afin de rendre possible la transmission (FAI etc..) ou qu'elles servent à une utilisation licite (cache d'un navigateur Internet etc…)
Lorsque l'acte de reproduction à un objet purement technique.

Droit de l'informatique, droit d'auteur et logiciel

I. Qu'est-ce qu'un logiciel au sens de la loi ?

Le Code de la propriété intellectuelle ne donne pas de définition du logiciel.

Il mentionne néanmoins le logiciel dans son article L. 112-2 qui donne une liste des œuvres protégées. « *Sont considérés notamment comme œuvres de l'esprit au sens du présent Code :…13° (Loi n°94-361 du 10 mai 1994) les logiciels, y compris le matériel de conception préparatoire* ».

Le logiciel est donc protégeable comme une œuvre de l'esprit par le droit d'auteur.

A. Le droit moral sur un logiciel

Logiciel, droit moral édulcoré au détriment de l'auteur

Le droit moral a, comme nous avons pu le voir précédemment, été créé dans le but de mieux protéger la personne du créateur et dans celui de permettre une meilleure maîtrise de la carrière de l'œuvre par ce dernier. Ce droit caractéristique du droit d'auteur est fortement mis à mal par les lois spécifiques intervenues en matière de logiciel. Le droit moral a en effet été, du fait de la convention de Berne en son article 6 bis, réduit à son strict minimum. L'article L. 46 de la loi du 3 juillet 1985, devenu l'article L. 121-7 du Code de la propriété intellectuelle, instaure, en effet, un régime dérogatoire à la loi de 1957, selon lequel **l'auteur ne peut sauf stipulation contraire, exercer son droit de repentir ou de retrait.**

Le droit de repentir et de retrait, normalement prévu à l'article L 121-4 du Code de la propriété intellectuelle n'est pas effectif pour les créateurs de logiciel. Il ne leur est donc pas possible de faire valoir, de mettre fin à sa diffusion, ni de retoucher celui-ci, au motif qu'ils auraient des regrets. Il leur est donc impossible de revenir sur le lancement sur le marché d'un logiciel.

Le cessionnaire d'un logiciel n'a donc pas, à l'inverse du cessionnaire d'une œuvre soumise au droit commun, à supporter une atteinte à son droit de propriété sur l'œuvre qu'il a acquise.

Le droit moral est si peu important en matière de logiciel, que la Cour d'appel de Douai[1] a affirmé que dans ce cas, le droit moral se réduit au droit au nom.

Quelques prérogatives accordées à l'utilisateur final

Par ailleurs et par exception en matière de logiciels, la loi accorde un certain nombre de prérogatives à l'utilisateur, sous réserve que leur exercice ne porte pas atteinte à l'exploitation normale du logiciel et ne cause pas un préjudice injustifié aux intérêts légitimes de l'auteur du logiciel.

---

[1] Douai, 1re ch., 1er juillet. 1996, JCP éd. E 1997, I, n°657, n°1, obs. Vivant et Le Stanc, PIBD 1997, n°627, III, p. 129.

Sauf à ce que l'auteur se soit réservé contractuellement ce droit, il est permis à l'utilisateur final de corriger les erreurs du logiciel.

L'utilisateur peut également faire une copie du logiciel à des fins de sauvegarde exclusivement. Cette exception est généralement interprétée de façon à ce qu'un utilisateur ne puisse réaliser qu'une seule copie de sauvegarde lorsque cela s'avère nécessaire pour résoudre d'éventuels problèmes. La copie ne sera pas autorisée si le producteur du logiciel a lui-même prévu dans le contrat qu'il s'engage à livrer lui-même cette copie de sauvegarde ou à résoudre personnellement tout problème auquel serait confronté l'utilisateur.

Dès lors, toute copie qui ne correspond pas à une copie de sauvegarde est illicite. La copie de sauvegarde doit être appréciée comme une tolérance et non comme un droit à part entière.

L'acquéreur du logiciel peut également étudier le fonctionnement du logiciel afin de déterminer les idées et principes qui en sont à la base.
Il ne sera autorisé à décompiler le programme qu'à des fins d'interopérabilité strictement encadrées par la loi.

Ces différentes exceptions au droit d'auteur ne seront accordées qu'à une personne détentrice des originaux (et non d'une copie non autorisée des originaux).

B. Les droits patrimoniaux sur un logiciel

En matière informatique, il est extrêmement rare qu'un auteur travaille de manière libre et inspirée à la création d'un logiciel. Il est très souvent un salarié qui travaille dans le cadre d'un contrat de travail conformément aux instructions d'un employeur.

Des éditeurs de logiciels éditent la grande majorité des programmes d'ordinateurs à la vente.

La qualification d'œuvre logiciel entraine dévolution automatique des droits patrimoniaux à l'éditeur.

C. A qui appartiennent les droits sur un logiciel créé dans le cadre d'un travail ?

S'agissant de la création de logiciels, l'article L.113-9 du code de propriété intellectuelle prévoit donc qu'il y a dévolution automatique des droits d'auteur à l'employeur, que le logiciel soit créé par le salarié dans l'exercice habituel de ses fonctions ou dans le cadre d'études qui lui sont spécifiquement confiées mais qui n'entrent pas dans son activité habituelle.

Cette disposition déroge au droit commun de la propriété littéraire et artistique pour attribuer ces droits à l'employeur au détriment du salarié.

Il faudra néanmoins remplir trois conditions préalables.

1) **Le créateur du logiciel devra être un salarié de l'entreprise,** ce qui exclut de fait les intérimaires, les développeurs employés par un prestataire externe ainsi que les stagiaires.

2) **Le créateur du logiciel devra avoir créé le logiciel dans l'exercice de ses fonctions ou d'après les instructions de son employeur.**

3) Par ailleurs, **aucune clause de son contrat de travail ne doit pas avoir pour effet de priver d'effet les dispositions précitées.**

A titre d'exemple concernant cette 3ème condition, *sachez que dans un jugement du 4 juin 2014, le Conseil des prud'hommes de Paris n'a pas remis en cause la validité d'une clause de propriété intellectuelle d'un contrat de travail imposant à l'employeur de publier des logiciels sous licence libre développés par des salariés. Cette clause s'inscrivait dans le cadre de l'article L. 113-9 du code de la propriété intellectuelle, qui prévoit la dévolution automatique à l'employeur des droits patrimoniaux sur les logiciels développés par des salariés, sauf stipulations contraires. Or, dans cette affaire, la société avait accordé au salarié la co-propriété du code source de certains logiciels identifiés. Mais l'originalité de cette clause réside surtout dans le fait qu'elle s'applique à des logiciels libres, reconnus comme tels par l'employeur. Il y est écrit que les logiciels seront co-signés par l'employeur et le salarié qui s'engagent à mettre le code source à disposition ainsi que le logiciel sous licence GPL. L'employeur a cependant voulu remettre cette clause en question mais le salarié concerné n'a jamais signé l'avenant. Considérant que son ex-employeur n'avait pas respecté cette clause imposant la publication du logiciel, il a saisi le conseil des prud'hommes, à l'instar de deux autres collègues dans le même cas. Les conseillers, en nombre pair, n'ayant pu se mettre d'accord, un juge départiteur est intervenu pour les départager. Ils n'ont cependant pas tranché le fond du litige, au motif que les logiciels concernés n'avaient pas été cités précisément, bien que la clause vise chacun d'entre eux nommément. Le salarié n'a pas fait appel de la décision. Par ailleurs, son ex-employeur est en liquidation judiciaire.*

Si ces trois conditions sont remplies, l'employeur sera alors investi des droits d'exploiter le logiciel à sa guise. On parlera alors de dévolution automatique des droits, par opposition au droit de la propriété littéraire et artistique dans lequel seul un contrat de cession entre l'auteur et son cessionnaire formalise la transmission effective des droits.

D. Quels sont les éléments du logiciel protégés par le droit d'auteur ?

La protection s'étend non seulement aux logiciels en tant que programmes (software), mais aussi au matériel de conception préparatoire et de façon générale à tous les travaux aboutissant au développement du programme à condition qu'ils soient de nature à permettre la réalisation du programme à un stade ultérieur.

Ce sont les séquences du programme qui bénéficient de la protection, c'est à dire les codes sources et les versions exécutables.

Par conséquent, il est permis de reprendre les mêmes solutions qu'un logiciel existant à condition que le nouveau logiciel soit complètement différent dans son architecture et dans son codage.

Important : Il ne suffira pas de modifier quelques lignes de code pour pouvoir prétendre ne pas avoir contrefait un logiciel et de la même manière. Il ne suffira pas de l'avoir fait pour pouvoir prétendre bénéficier à son tour d'un droit d'auteur eu égard au fait qu'on aurait rempli la condition d'originalité.

Certains éléments sont considérés comme des éléments informatiques à l'origine de la conception du logiciel qui ne présentent pas en tant que tels une forme. A ce titre, ils appartiennent au domaine de l'idée. Les idées étant de libre parcours, elles ne sont pas protégeables par le droit d'auteur.

Les éléments du logiciel non protégeables sont :

1. Les fonctionnalités
2. Les algorithmes
3. Les interfaces
4. Les langages de programmation

A l'inverse et à la condition de répondre à la condition d'originalité, sont protégeables :

1. L'architecture des programmes
2. Le code source
3. Le code objet (résultat de la compilation du code source)
4. Les différentes versions
5. Les écrans et modalités d'interactivité
6. Le matériel de conception préparatoire : ébauches, maquettes, prototypes, etc…)

E. Quid de la brevetabilité du logiciel ?

Certains pays parmi lesquels les Etats-Unis et le Japon possèdent des réglementations permettant l'octroi de brevets sur les logiciels.

En Europe, les législations des pays membres de l'Union européenne n'autorisent, pour la plupart, pas la délivrance de brevets pour « les logiciels en tant que tels ».
En pratique, des brevets sont possibles et accordés pour les inventions mises en œuvre par l'intermédiaire d'un logiciel, c'est-à-dire quand le logiciel est lié à un système physique ayant un effet technique.

Dans ce cas, c'est le résultat qui est brevetable et non pas le logiciel stricto sensu.

La question de la brevetabilité du logiciel fait actuellement l'objet d'un vif débat entre les différents pays de l'Union Européenne afin d'harmoniser les différentes législations et de clore le débat définitivement.

En France, il n'y a pas de brevet de logiciel. Seul le droit d'auteur a vocation à s'appliquer. Puisque le droit d'auteur existe depuis la création de l'œuvre, Il sera déterminant d'apporter la preuve que le logiciel que vous prétendez avoir créé l'a été à partir d'une date certaine (enveloppe Soleau, dépôt électronique par horodatage des codes sources).

F. Qu'est-ce qu'un logiciel libre ?

Contrairement à ce que l'on peut penser de prime abord, le logiciel libre est compatible avec le droit et le droit français en particulier.

L'un des logiciels libres les plus connus est celui qui est offert par le biais de la célèbre Licence publique générale (GNU) ou General Public License, communément abrégé GNU GPL voire « GPL ».

Comme toute licence, conçue comme un droit d'utilisation d'un bien ou d'une œuvre (une sorte de location ou de droit d'usage) GNU GPL est une licence qui fixe les conditions légales de distributions de logiciels du projet GNU.

Même en dehors du projet GNU, cette licence a été adoptée comme le document référence définissant le mode d'utilisation, d'usage et de diffusion par de nombreux auteurs de logiciels libres.

1. Conciliation entre GNU GPL et droit d'auteur

Il n'est pas exact d'opposer systématiquement GNU et droit d'auteur.
La GPL a adopté la notion de Copyleft (subtil jeu de mot censé la distinguer du copyright – pendant anglo-saxon du droit d'auteur français).

Le Copyleft, comme le droit d'auteur ont vocation à définir et à encadrer les droits des utilisateurs de façon contraignante. Même si le mécanisme est très voisin, c'est l'objectif poursuivi qui diffère.

Nous avons pu voir précédemment que les droits patrimoniaux et moraux du droit d'auteur ont surtout pour objectif de protéger au mieux l'auteur et l'œuvre qu'il a créée ; Les utilisateurs n'ont qu'un droit à la copie de sauvegarde du logiciel.

Le Copyleft se concentre tout particulièrement sur le droit des utilisateurs. Il vise à leur accorder le droit d'utiliser, d'étudier, de modifier et de diffuser le logiciel et ses versions dérivées.

Là où vous seriez immédiatement attaquables pour contrefaçon devant les tribunaux dans l'hypothèse où vous modifieriez un logiciel lambda sans l'autorisation expresse de son auteur, le Copyleft prévu par le GPL vous permet de le faire à la condition de respecter un certain nombre de conditions.

L'idée d'un travail collaboratif ou contributif est sous jacente de la licence GPL.

2. Les principaux termes de la licence GPL

En acceptant la licence GPL, toute personne est à même de recevoir une copie d'un travail sous GPL.
Elle obtient le droit de modifier le travail, de l'étudier, de le redistribuer ou d'en redistribuer un modifié ou dérivé.

Le travail sous logiciel libre GPL peut être gratuit ou rémunéré à l'inverse d'autres licences qui interdisent la redistribution dans un but commercial.
En cas de modification du travail, le travail réalisé par le licencié doit impérativement être placé sous la même licence ce qui signifie qu'il devra accorder le droit (pour quelqu'un d'autre) de modifier le travail, de l'étudier, de le redistribuer ou d'en redistribuer un modifié ou dérivé.

Le droit de redistribuer ne sera garanti si et seulement si l'utilisateur fournit le code source de la version modifiée.
Il faut se soumettre aux conditions du Copyleft pour pouvoir bénéficier des droits de modifier et de redistribution interdits par le copyright et le droit d'auteur, mais permis par le Copyleft.

Si cette condition n'est pas respectée, il s'agira d'une contrefaçon.

De nombreux distributeurs de programmes fournissent les codes sources avec l'exécutable, mais la condition de fournitures des codes sources pourra être considérée comme remplie si lesdits codes sont fournis sur demande par le biais d'un CD ou encore sur internet par FTP, CVS etc…

Si on décide de modifier pour son compte personnel sans songer à redistribuer, l'obligation de communiquer les codes sources ne s'appliquent pas au motif que le Copyleft s'applique uniquement quand une personne a l'intention de redistribuer le programme.

Une version modifiée privée d'un CMS de site internet, par exemple, ne sera pas obligée de livrer ses codes sources à la condition que cette version ne soit pas redistribuée. Si elle venait à l'être, il faudrait alors donner accès aux codes sources.

Le Tribunal de grande instance de Paris a jugé applicable la licence GPL (version 2) en France) par un jugement du 28 mars 2007.

Le litige portait sur un logiciel qui intégrait sans droit un logiciel sous licence GPL.
Le Tribunal a retenu à propos du logiciel dérivé que : « Ce programme a la particularité de dépendre de la licence GNU qui permet une utilisation libre du logiciel mais requiert une licence si le travail basé sur le programme ne peut être identifié comme raisonnablement indépendant et doit être considéré comme dérivé du programme litigieux.

En conclusion, contrairement à l'idée reçue, le logiciel libre ne contrevient pas aux principes du droit d'auteur, mais, au contraire, exploite ceux-ci afin de garantir la libre circulation du code source modifié par les divers développeurs.

Le principe même des licences libres procède d'un paradoxe qui implique d'utiliser le droit d'auteur pour aboutir à une libre reproduction, résultat inverse au principe de restriction et d'autorisation accordé par le monopole du droit d'auteur.

Ce n'est pour autant pas une négation du droit d'auteur puisque la licence libre l'utilise pour arriver au résultat escompté.

Préambule

Qu'est-ce qu'une donnée à caractère personnel ?

L'article 2 alinéa 2 de la loi informatique et libertés dispose que :

« Constitue une donnée à caractère personnel toute information relative à une personne physique identifiée ou qui peut être identifiée, directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments qui lui sont propres. Pour déterminer si une personne est identifiable, il convient de considérer l'ensemble des moyens en vue de permettre son identification dont dispose ou auxquels peut avoir accès le responsable du traitement ou toute autre personne ». ex. : nom, n° d'immatriculation, n° de téléphone, photographie, éléments biométriques tels que l'empreinte digitale, ADN, informations permettant de discriminer une personne au sein d'une population telles que, par exemple, le lieu de résidence, la profession, le sexe, l'âge, etc.).

Il peut en effet s'agir d'informations qui ne sont pas associées au nom d'une personne mais qui peuvent permettre de l'identifier et de connaître ses habitudes ou ses goûts. Exemples : « Le propriétaire du véhicule 3636AB75 est abonné à telle revue » ou encore « l'assuré social 1600530189196 va chez le médecin plus d'une fois par mois ».

Qu'est-ce qu'une donnée sensible ?

Parmi les données à caractère personnel, il existe une sous-distinction liée aux données sensibles. Les données sensibles sont celles qui font apparaître, directement ou indirectement, les origines raciales ou ethniques, les opinions politiques, philosophiques ou religieuses ou l'appartenance syndicale des personnes, ou sont relatives à la santé ou à la vie sexuelle de celles-ci. Par principe, la collecte et le traitement de ces données sont interdits. Cependant, dans la mesure où la finalité du traitement l'exige, les traitements pour lesquels la personne concernée a donné son consentement exprès et les traitements justifiés par un intérêt public après autorisation de la CNIL ou décret en Conseil d'Etat ne seront pas soumis à cette interdiction.

Qu'est-ce qu'un traitement de données à caractère personnel ?

L'article 2 alinéa 3 de la loi informatique et libertés dispose que : « Constitue un traitement de données à caractère personnel toute opération ou tout ensemble d'opérations portant sur de telles données, quel que soit le procédé utilisé, et notamment la collecte, l'enregistrement, l'organisation, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, ainsi que le verrouillage, l'effacement ou

la destruction ».

Gros plan sur les 5 grands principes à respecter en matière de données à caractère personnel

Avant de parler du RGPD en général, il est utile de revenir sur ce qui constitue, depuis la loi dite informatique et libertés de 1978, le socle des principes en matière de données à caractère personnel repris dans le texte européen qu'est le RGPD.

L'article 6 du RGPD dispose, en effet, que : «

« 1. Les données à caractère personnel doivent être :

a) **traitées de manière licite, loyale et transparente au regard de la personne concernée (licéité, loyauté, transparence);**

b) **collectées pour des finalités déterminées, explicites et légitimes, et ne pas être traitées ultérieurement d'une manière incompatible avec ces finalités;** le traitement ultérieur à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques n'est pas considéré, conformément à l'article 89, paragraphe 1, comme incompatible avec les finalités initiales (limitation des finalités);

c) **adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées (minimisation des données);**

d) **exactes et, si nécessaire, tenues à jour; toutes les mesures raisonnables doivent être prises pour que les données à caractère personnel qui sont inexactes, eu égard aux finalités pour lesquelles elles sont traitées, soient effacées ou rectifiées sans tarder (exactitude);**

e) **conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire au regard des finalités pour lesquelles elles sont traitées;** les données à caractère personnel peuvent être conservées pour des durées plus longues dans la mesure où elles seront traitées exclusivement à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques conformément à l'article 89, paragraphe 1, pour autant que soient mises en œuvre les mesures techniques et organisationnelles appropriées requises par le présent règlement afin de garantir les droits et libertés de la personne concernée **(limitation de la conservation);**

f) **traitées de façon à garantir une sécurité appropriée des données à caractère personnel, y compris la protection contre le traitement non autorisé ou illicite et contre la perte, la destruction ou les dégâts d'origine accidentelle, à l'aide de mesures techniques ou organisationnelles appropriées (intégrité et confidentialité);** »

La loi *« Informatique et Libertés »* et le RGPD ont donc défini les principes à respecter lors de la collecte, du traitement et de la conservation de ces données. La loi prévoit également un certain nombre de droits pour les personnes dont les données personnelles ont été recueillies.

1. **Le principe de finalité : une utilisation encadrée des fichiers**

Ce principe implique que les données à caractère personnel ne peuvent être recueillies et traitées que pour un usage déterminé et légitime, correspondant aux missions de l'entreprise ou de la personne physique responsable du traitement.

Le fichier ainsi constitué ne peut donc être utilisé à des fins commerciales ou politiques, sauf accord exprès du client ou de la personne.

Ce principe implique que les informations exploitées dans un fichier soient cohérentes par rapport à son objectif.

Ces données ne peuvent pas être réutilisées de manière incompatible avec la finalité pour laquelle elles ont été collectées.

Tout détournement de finalité est passible de 5 ans d'emprisonnement et de 300 000 euros d'amende.

> L'article 226-21 du Code pénal dispose, en effet, que : « Le *fait, par toute personne détentrice de données à caractère personnel à l'occasion de leur enregistrement, de leur classement, de leur transmission ou de toute autre forme de traitement, de détourner ces informations de leur finalité telle que définie par la disposition législative, l'acte réglementaire ou la décision de la Commission nationale de l'informatique et des libertés autorisant le traitement automatisé, ou par les déclarations préalables à la mise en oeuvre de ce traitement, est puni de cinq ans d'emprisonnement et de 300 000 euros d'amende* ».

Le principe de finalités déterminées est donc au cœur de la confiance que les personnes peuvent avoir dans les services de la société numérique. C'est grâce à ce principe que les données personnelles ne sont pas des marchandises comme les autres.

2. **Le principe de minimisation**

Ce principe découle directement du principe de finalité.

Il impose que seules doivent être enregistrées les informations et données personnelles adéquates, pertinentes et nécessaires pour assurer la mission poursuivie par l'entreprise.

Toutes celles qui ne sont pas en rapport avec cette mission seront considérées comme contraire aux principes de pertinence et de proportionnalité.

Il faut que la donnée collectée fasse corps avec le domaine d'activité de l'entreprise ou à défaut avec quelque chose dont cette entreprise pourrait légitimement indiquer à la CNIL qu'elle en avait besoin pour améliorer son service.

3. **Le principe de durée limitée de conservation des données**

Les informations ne peuvent être conservées de façon indéfinie dans les fichiers informatiques. Une durée de conservation raisonnable doit être, le plus souvent, établie en fonction de la finalité de chaque fichier.

La CNIL préconise notamment une durée n'excédant pas 3 ans pour les données à caractère marketing et commercial relative à des prospects ou anciens clients. **Elles ne peuvent être conservées que pendant un délai de trois ans à compter de leur collecte par le responsable de traitement ou du dernier contact émanant du prospect.**

Au terme de ce délai de trois ans, le responsable de traitement peut reprendre contact avec la personne concernée afin de savoir si elle souhaite continuer à recevoir des sollicitations commerciales. En l'absence de réponse positive et explicite de la personne, les données devront être supprimées ou archivées conformément aux dispositions en vigueur et notamment celles prévues par le code de commerce, le code civil et le code de la consommation.

Le code pénal sanctionne la conservation des données pour une durée supérieure à celle qui a été déclarée de 5 ans d'emprisonnement et de 300 000 euros d'amende (article 226-20 du Code pénal).

Cela implique donc, dans l'hypothèse, d'une utilisation de donnée personnelle d'être en mesure de supprimer celles qui par l'effet du temps doivent l'être et de ne conserver que celles qui peuvent continuer à être traitées.

4. Le principe de sécurité et de confidentialité

1.1 Sécurité

L'article 32 du RGPD intitulé « sécurité du traitement » dispose que : *« Compte tenu de l'état des connaissances, des coûts de mise en œuvre et de la nature, de la portée, du contexte et des finalités du traitement ainsi que des risques, dont le degré de probabilité et de gravité varie, pour les droits et libertés des personnes physiques,* ***le responsable du traitement et le sous-traitant mettent en œuvre les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque, y compris entre autres, selon les besoins*** *».*

En somme, il s'agit de comprendre que plus la sensibilité de la donnée sera avérée (ex : données médicales) et plus les mesures de sécurité attendues seront accrues. A l'inverse, des données personnelles classiques gérées par des sociétés tout aussi anodines pourront n'appeler que les mesures de sécurité élémentaires.

De façon générale, le responsable du traitement, est astreint à une obligation de sécurité : il doit prendre les mesures nécessaires pour garantir la confidentialité des données et éviter leur divulgation.

Les données contenues dans les fichiers ne peuvent être consultées que par les services habilités à y accéder en raison de leurs fonctions.

Il faut NOTAMMENT que l'entreprise veille à ce que chaque utilisateur ait un mot de passe individuel régulièrement changé et que les modalités d'accès soient précisément définies en fonction des besoins réels.

Le responsable du traitement doit prendre toutes les mesures pour empêcher que les données

soient déformées, endommagées ou que des tiers non autorisés y aient accès.

Exemple : S'il est fait appel à un prestataire externe, des garanties contractuelles doivent être envisagées.

Tout responsable de traitement informatique de données personnelles **doit adopter des mesures de sécurité physiques** (sécurité des locaux), **logiques** (sécurité des systèmes d'information) et **adaptées** à la nature des données et aux risques présentés par le traitement. Exemple : Protection anti-incendie, copies de sauvegarde, installation de logiciel antivirus, changement fréquent des mots de passe alphanumériques d'un minimum de 8 caractères.

Les mesures de sécurité doivent être adaptées à la nature des données et aux risques présentés par le traitement (Les banques et les opérateurs de télécommunications sont tenus à des mesures de sécurité plus importantes et plus lourdes qu'une PME.

Exemple : Authentification forte pour l'accès aux résultats d'examen, chiffrement des coordonnées bancaires transitant sur internet.

Le non-respect de l'obligation de sécurité est sanctionné de 5 ans d'emprisonnement et de 300 000 euros d'amende (Article 226-17 du Code pénal).

4.2 Confidentialité

Seules les personnes autorisées peuvent accéder aux données personnelles contenues dans un fichier.

Il s'agit des destinataires explicitement désignés pour en obtenir régulièrement communication et des «tiers autorisés» ayant qualité pour les recevoir de façon ponctuelle et motivée (ex. : la police, le fisc).

La communication d'informations à des personnes non-autorisées est punie de 5 ans d'emprisonnement et de 300 000 euros d'amende (article 226-22 du Code pénal).

Il est hors de question pour une entreprise de transmettre les données personnelles de ses utilisateurs ou clients à une entité tierce (effet relatif des conventions l'impose au même titre que le principe de confidentialité imposé par la loi de 1978).

Si un contrat de gestion des données devait être conclu avec un prestataire externe à l'entreprise, il conviendrait de lui faire assumer cette obligation de confidentialité et de bien préciser le périmètre de la mission qui l'autorise à gérer à son tour (en tant que co-responsable du traitement des données à caractère personnel) lesdites données.

La divulgation d'informations commise par imprudence ou négligence est punie de 3 ans d'emprisonnement et de 100 000 euros d'amende.

5. Le principe du respect du droit des personnes (obligation de transparence)

L'article 13 du RGPD dispose que :

« Lorsque des données à caractère personnel relatives à une personne concernée sont collectées auprès de cette personne, le responsable du traitement lui fournit, au moment où les données en question sont obtenues, toutes les informations suivantes :

a) l'identité et les coordonnées du responsable du traitement et, le cas échéant, du représentant du responsable du traitement

b) le cas échéant, les coordonnées du délégué à la protection des données;

c) les finalités du traitement auquel sont destinées les données à caractère personnel ainsi que la base juridique du traitement;

d) lorsque le traitement est fondé sur l'article 6, paragraphe 1, point f), les intérêts légitimes poursuivis par le responsable du traitement ou par un tiers;

e) les destinataires ou les catégories de destinataires des données à caractère personnel, s'ils existent; et

f) le cas échéant, le fait que le responsable du traitement a l'intention d'effectuer un transfert de données à caractère personnel vers un pays tiers ou à une organisation internationale, et l'existence ou l'absence d'une décision d'adéquation rendue par la Commission ou, dans le cas des transferts visés à l'article 46 ou 47, ou à l'article 49, paragraphe 1, deuxième alinéa, la référence aux garanties appropriées ou adaptées et les moyens d'en obtenir une copie ou l'endroit où elles ont été mises à disposition; »

Le responsable d'un fichier doit donc permettre aux personnes concernées par des informations qu'il détient d'exercer pleinement leurs droits. Pour cela, il doit leur communiquer : son identité, la finalité de son traitement, le caractère obligatoire ou facultatif des réponses, les destinataires des informations, l'existence de droits, les transmissions envisagées.

Le refus ou l'entrave au bon exercice des droits des personnes est puni de 1500 euros par infraction constatée et 3 000 euros en cas de récidive. (Article 110 du décret du 20 octobre 2005 et article 131-13 du Code pénal).

a) Informer les intéressés (article 13 du RGPD)

Lorsque les données sont recueillies par exemple par voie de questionnaire, les usagers concernés et le personnel de l'entreprise doivent être informés de la finalité du traitement du caractère obligatoire ou facultatif du recueil, des destinataires des données et des modalités d'exercice des droits qui leur sont ouverts au titre de la loi *« Informatique et Libertés »* : droit d'accès et de rectification mais aussi, droit de s'opposer, sous certaines conditions, à l'utilisation de leurs données.

L'article 15 du RGPD reconnait un droit pour la personne concernée par le traitement « de demander au responsable du traitement la rectification ou l'effacement de données à caractère personnel, ou une limitation du traitement (...), ou du droit de s'opposer à ce traitement ».

b) Les droits d'accès et de rectification (article 39 de la loi informatique et libertés et

article 15 du RGPD)

Toute personne peut demander communication de toutes les informations la concernant contenues dans un fichier détenu par l'entreprise et a le droit de faire rectifier ou supprimer les informations erronées.

Toute personne peut demander la rectification des informations inexactes la concernant. Le droit de rectification complète le droit d'accès.
Il permet d'éviter qu'un organisme ne traite ou ne diffuse de fausses informations sur vous.

c) Le droit d'opposition ou de limitation du traitement (article 38 de la loi informatique et libertés et article 15 du RGPD)

Toute personne a le droit de s'opposer, pour des motifs légitimes, à ce que des données la concernant soient enregistrées dans un fichier informatique, sauf si celui-ci présente un caractère obligatoire.

Vous pouvez donc vous opposer à ce que les données vous concernant soient diffusées, transmises ou conservées. Le droit d'opposition s'entend donc également comme un droit de suppression.

Focus sur le RGPD

Le Règlement n°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 (ci-après RGPD) a pour finalité de remplacer la directive 95/46/CE et instaurer un cadre général et unique pour la protection des données en Europe.

Sur proposition de la Commission européenne en date du 25 janvier 2012, ce Règlement a été adopté conjointement par le Parlement européen et le Conseil et est applicable depuis le 25 mai 2018.

Il convient d'abord de préciser que ce Règlement européen applicable depuis le 25 mai 2018, est, par essence, d'application directe dans tous les Etats membres de l'Union européenne, c'est à dire sans qu'il soit nécessaire d'attendre une quelconque transposition (à l'inverse de la Directive).

Une loi en date du 20 juin 2018 est venue modifiée la loi informatique et libertés de 1978 afin qu'elle mette en adéquation les dispositions du Règlement avec la loi française applicable tout en précisant des points pour lesquels le Règlement renvoie explicitement au Droit des Etats membres (notamment concernant les données sensibles).

- **Un texte qui harmonise les législations européennes en matière de respect des données à caractère personnel**

Parce que la précédente règlementation[1] (issue d'une Directive en date du 24 octobre 1995) n'était plus adaptée aux enjeux économiques et juridiques liés à l'exploitation des données personnelles par les acteurs du monde du numérique, parce qu'il convenait qu'un texte vienne durcir les contraintes et sanctions en la matière et surtout parce que ce texte imposera aux Etats membres de l'Union européenne des dispositions communes en vue de remplacer les règlementations nationales qui présentent actuellement des disparités significatives, la promulgation du Règlement général sur la protection des données **(ci-après le « RGPD » ou le «Règlement »)**[2] devenait une nécessité.

- **Un texte avec un champ d'application dépassant les frontières de l'Union européenne**

Le RGPD a vocation à s'appliquer aux traitements de données à caractère personnel qui ont lieu sur le territoire de l'Union Européenne, à ceux qui touchent des ressortissants européens (même lorsque le traitement a lieu hors UE), mais aussi à ceux pour qui le responsable de

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

[2] Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE

traitement (i.e. « data controller ») et/ou le sous-traitant (i.e. « data processor ») sont établis sur le territoire de l'Union européenne.

- **Un texte applicable depuis le 25 mai 2018**

Si le RGPD est entré en vigueur le 27 avril 2016, sa mise en application est effective depuis le 25 mai 2018. Les entreprises devront, au plus tard à cette date, être en conformité avec le Règlement. Celle qui sont l'objet de poursuite pour des faits constatés avant cette date se verront sanctionnées sur la base de l'ancienne règlementation sur la base du principe d'application de la loi dans le temps.

- **Un texte visant à une meilleure protection des personnes concernées**

L'objectif principal du RGPD est d'assurer une meilleure protection des personnes concernées par les traitements de données à caractère personnel ainsi que la sécurité, l'intégrité, la confidentialité et la nécessité desdits traitements et de l'utilisation des données à caractère personnel.

En conséquence, le Règlement vient, de façon générale, renforcer certaines dispositions qui existent déjà, notamment, au niveau de la législation française via la loi informatique et libertés du 6 janvier 1978 modifiée, créer de nouvelles obligations pour le responsable du traitement (i.e. la personne physique ou morale qui détermine les finalités et les moyens de toute opération appliquée à des données à caractère personnel et pour le compte de laquelle est réalisée le traitement) tout comme pour les sous-traitants (i.e. les personnes qui traitent les données à caractère personnel uniquement pour le compte et sur les instructions du responsable de traitement) et enfin changer la manière dont les différents acteurs doivent appréhender leur politique en matière de traitement et gestion des données à caractère personnel pour se conformer aux exigences règlementaires.

- **Une mise à jour significative et ambitieuse du barème des sanctions**

L'une des raisons pour lesquelles le RGPD fait tant parler tient au fait qu'il prévoit des amendes maximales, pour non-respect des dispositions légales, qui dépassent largement les standards actuels en vigueur en France, même si les sanctions, qui étaient jusqu'il y a peu de temps assez faibles, (jusqu'à 150 000 euros d'amende) ont été revues à la hausse depuis la loi pour la République Numérique du 7 octobre 2016 (jusqu'à 3 millions d'euros).

Ceux qui contreviendront au RGPD s'exposeront à des amendes qui pourront varier en fonction du type d'infraction. Elles pourront s'élever jusqu'à 10 millions d'euros ou, dans le cas d'une entreprise, jusqu'à 2% du chiffre d'affaires annuel mondial total de l'exercice précédent, le montant le plus élevé pouvant être retenu (*exemples : absence de protection des données dès la conception, non-respect de la désignation d'un DPD)* voire selon un autre type d'infraction jusqu'à 20 millions d'euros ou, dans le cas d'une entreprise, jusqu'à 4% du chiffre d'affaires annuel mondial total de l'exercice précédent, le montant le plus élevé pouvant être retenu (exemples : *infraction relative aux transferts des données ou aux non-respect des règles du consentement au traitement*).

Ces sanctions sont désormais susceptibles de faire peur aussi bien aux grandes entreprises qu'aux PME/TPE, et ce d'autant plus que depuis la loi pour une république numérique du 7 octobre 2016, il est possible, en France, de sanctionner les entreprises sans mise en demeure préalable quand le manquement constaté ne peut faire l'objet d'une mise en conformité dans le cadre d'une mise en demeure, la CNIL pourra prononcer directement des sanctions pécuniaires (article 65).

- **Des obligations étendues et des droits renforcés**

Le RGPD renforce le droit des personnes à travers les notions, déjà existantes en France, d'accès, de rectification et d'opposition tout en créant un droit de suppression renforcé, qualifié de droit à l'oubli, opposable au responsable du traitement notamment quand les données ne sont plus nécessaires au regard de la finalité pour lesquelles elles ont été collectées ainsi que d'un droit à la portabilité (au sens d'une disposition visant à permettre aux personnes de récupérer les données personnelles les concernant qu'elles avaient, elles-mêmes, transmises au responsable du traitement).

Le RGPD impose, à l'instar de la loi informatique et libertés de 1978 modifiée, que le respect des droits des personnes passe par le fait pour le responsable du traitement de s'assurer que le traitement qu'il met en œuvre soit **licite**, (au sens où il doit être soit consenti par la personne concernée, soit nécessaire à l'exécution du contrat signé par cette personne, soit découler du respect d'une obligation légale, soit d'un intérêt légitime du responsable du travail du traitement qui ne devra pas être inférieur aux intérêts de la personne concernée).

Il devra également vérifier que le traitement est **loyal**. Ainsi, seules les données adéquates, nécessaires et pertinentes devront être collectées et ce selon des finalités déterminées, explicites et légitimes (transposition du principe de proportionnalité présent dans la loi informatique et libertés de 1978 modifiée).

Le responsable du traitement devra **obtenir un consentement de la personne concernée** lequel se devra d'être « *un acte positif clair par lequel la personne concernée manifeste de façon libre, spécifique, éclairée et univoque son accord au traitement des données à caractère personnel la concernant* ».

Cette exigence interdit de considérer le silence ou l'absence d'opposition (au sens d'une inaction) comme un consentement univoque et oblige les responsables de traitement à recueillir et conserver les éléments de preuve démontrant l'acte positif manifestant le consentement aussi bien sous forme électronique, par voie orale, par écrit ou par tout autre moyen. (ex : une case à cocher sur un site web accompagnée d'un texte manifestant ce consentement libre et éclairé).

La question de la durée du traitement est également abordée par le RGPD. Il prévoit que les données des personnes ne doivent être conservées que pour la durée strictement nécessaire au but poursuivi par le responsable du traitement. Dès lors, à l'issue de ce délai, le responsable du traitement devra s'assurer que les données soient détruites ou anonymisées, de sorte, dans le second cas évoqué, qu'il soit impossible d'associer cette donnée à une personne déterminée.

- **Quid des transferts de données hors de l'Union européenne ?**

Le RGPD reprend en substance la règlementation actuelle s'agissant de l'encadrement des transferts de données à caractère personnel hors de l'Union Européenne et de l'Espace Economique Européen.

Lesdits transferts seront autorisés à la condition d'être fondés, sur une décision d'adéquation, sur des garanties appropriées, qu'ils prennent la forme de règles d'entreprise contraignantes, ou qu'ils résultent de situations particulières (clauses contractuelles types dites CCT ou BCR Binding corporate rules / règles contraignantes d'entreprises).

Les Clauses Contractuelles Types sont des modèles de contrats de transfert de données personnelles adoptés par la Commission européenne.

Les Binding Corporate Rules (BCR) désignent une politique de protection des données intra-groupe en matière de transferts de données personnelles hors de l'Union européenne. Elles sont juridiquement contraignantes et respectées par les entités signataires du groupe, quel que soit leur pays d'implantation, ainsi que par tous leurs salariés d'une même entreprise ou d'un même groupe.

La différence majeure avec le cadre juridique actuel tient essentiellement dans le fait qu'à terme, les pays étant considérés comme assurant un niveau de protection adéquat (i.e. les pays situés hors du territoire de l'Union Européen mais pour lesquels les transferts de données à caractère personnel étaient autorisés) ne seront plus fixés individuellement par les Etats-Membres, mais par la Commission européenne.

Nous allons aborder successivement la question du passage d'un système de formalités préalables au traitement au principe d'accountability (I), le développement des exigences liées à la sécurité des données inhérent au RGPD (II) et enfin l'obligation de désigner un Délégué à la protection des données (ci-après « DPD » ou « Data protection officer - DPO ») (III).

I. Un changement par rapport à la politique de traitement des données à caractère personnel actuellement en vigueur

Le RGPD instaure une nouvelle façon d'aborder les obligations relatives au traitement des données à caractère personnel par le responsable dudit traitement.

A. Un changement de paradigme

Ce changement que met en œuvre le RGPD tient notamment au fait qu'il supprime (mis à part quelques cas spécifiques) l'exigence de déclarations préalables au traitement (déclaration simplifiée, normale, demande d'avis, demande d'autorisation préalable) en faisant désormais peser sur le responsable du traitement la responsabilité de mettre en place les mesures techniques et fonctionnelles appropriées afin d'être en conformité avec le RGPD.

Il peut s'agir notamment de la mise en place de politique interne de gestion des données à caractère personnel, de mesures liées aux outils informatiques qui traitent ces données, ainsi que de mesures de traçabilité visant à démontrer à l'autorité nationale qu'elles ont bel et bien été mises en œuvre.

En tout état de cause, le responsable de traitement ainsi que le sous-traitant des traitements de données à caractère personnel devront tenir un registre de traitements indiquant à minima la finalité du traitement, les mesures mises en œuvre pour assurer la sécurité, la confidentialité et l'intégrité des données à caractère personnel, la durée de conservation des données à caractère personnel ainsi que les personnes ayant accès auxdites données et le tenir à la disposition de la CNIL en cas de contrôle (article 30 du RGPD).

L'article 30 du RGPD qui dispose que :

> *« Chaque responsable du traitement et, le cas échéant, le représentant du responsable du traitement tiennent un registre des activités de traitement effectuées sous leur responsabilité. Ce registre comporte toutes les informations suivantes:*
> *a) le nom et les coordonnées du responsable du traitement et, le cas échéant, du responsable conjoint du traitement, du représentant du responsable du traitement et du délégué à la protection des données;*
> *b) les finalités du traitement;*
> *c) une description des catégories de personnes concernées et des catégories de données à caractère personnel;*
> *d) les catégories de destinataires auxquels les données à caractère personnel ont été ou seront communiquées, y compris les destinataires dans des pays tiers ou des organisations internationales;*
> *e) le cas échéant, les transferts de données à caractère personnel vers un pays tiers ou à une organisation internationale, y compris l'identification de ce pays tiers ou de cette organisation internationale et, dans le cas des transferts visés à l'article 49, paragraphe 1, deuxième alinéa, les documents attestant de l'existence de garanties appropriées;*
> *f) dans la mesure du possible, les délais prévus pour l'effacement des différentes catégories de données;*
> *g) dans la mesure du possible, une description générale des mesures de sécurité techniques et organisationnelles visées à l'article 32, paragraphe 1 ».*

Ces registres répondent donc notamment aux questions suivantes :

- QUI ? (Le nom et les coordonnées du responsable du traitement (et de son représentant légal) et, le cas échéant, du délégué à la protection des données ; Catégories de données traitées
- POURQUOI ? La ou les finalités pour lesquelles sont collectées ou traitées ces données
- OÙ ? Lieu où les données sont hébergées. Dans quels pays les données sont éventuellement transférées.
- JUSQU'À QUAND ? Pour chaque catégorie des données, combien de temps sont-t-elles conservées.

- COMMENT ? Quelles mesures de sécurité sont mises en œuvre pour minimiser les risques.

B. Privacy by design / privacy by default

C'est ce même principe d'accountability ou de « responsabilisation » qui implique que le responsable du traitement comme le sous-traitant soient tenus, dès la conception des produits et services, de mettre en œuvre un socle protecteur des données à caractère personnel (notion dite de « ***privacy by design »***).

De la même façon, ils devront s'assurer que sans l'intervention préalable des personnes physiques concernées, les données à caractère personnel ne peuvent être rendues accessibles à un nombre indéterminé de personnes physiques et, que soient collectées et traitées uniquement des données à caractère personnel pertinentes au regard de la finalité du traitement considéré (notion dite de « ***privacy by default »*** (article 25 § 2).

le Privacy by design (sécurité dès la conception) consiste donc à mettre en œuvre, dès la conception des produits et services, un socle protecteur des données à caractère personnel. Cela signifie par exemple que le concepteur du logiciel devra avoir pensé au respect des données à caractère personnel dès la conception dudit produit afin de ne pas mettre en difficulté l'utilisateur (client).

Le Privacy by default (sécurité par défaut) consiste quant à lui au fait de restreindre l'accès aux données personnelles à des personnes déterminées et ne collecter que les données pertinentes au regard de la finalité du traitement. Il faut que dans l'utilisation du logiciel, le responsable du traitement s'assure que seules les personnes habilitées par leurs fonctions à avoir accès à une donnée puissent y avoir accès (authentification/droit d'accès/habilitation).

II. D'importantes attentes en matière de sécurité

Le responsable du traitement ainsi que son sous-traitant sont tenus de mettre en œuvre des mesures de sécurité appropriées aux données qu'ils collectent.

L'article 32.1 du RGPD dispose que : « *Compte tenu de l'état des connaissances, des coûts de mise en œuvre et de la nature, de la portée, du contexte et des finalités du traitement ainsi que des risques, dont le degré de probabilité et de gravité varie, pour les droits et libertés des personnes physiques, le responsable du traitement et le sous-traitant mettent en œuvre les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque, y compris entre autres, selon les besoins: a) la pseudonymisation et le chiffrement des données à caractère personnel; b) des moyens permettant de garantir la confidentialité, l'intégrité, la disponibilité et la résilience constantes des systèmes et des services de traitement; c) des moyens permettant de rétablir la disponibilité des données à caractère personnel et l'accès à celles-ci dans des délais appropriés en cas d'incident physique ou technique; d) une procédure visant à tester, à analyser et à évaluer régulièrement l'efficacité des mesures techniques et organisationnelles pour assurer la sécurité du traitement* ».

L'article 32.2 précise que : « *Lors de l'évaluation du niveau de sécurité approprié, il est tenu compte en particulier des risques que présente le traitement, résultant notamment de la destruction, de la perte, de l'altération, de la divulgation non autorisée de données à caractère personnel transmises, conservées ou traitées d'une autre manière, ou de l'accès non autorisé à de telles données, de manière accidentelle ou illicite* ».

Il existe un caractère subjectif réel dans l'appréciation que vous ferez des mesures de sécurité à mettre en oeuvre conformément à l'article 32 du RGPD (nature des données traitées, sensibilité de la donnée, domaine d'activité du responsable de traitement, état de l'art en matière de sécurité, mesures jugées élémentaires, etc..).

Parmi les quelques mesures qu'il est possible de citer comme élémentaires :

- que les supports sur lesquels reposent les traitements de données à caractère personnel ont été recensés.
- que des mesures de sécurité (physique) sont mises en œuvre pour empêcher que les données à caractère personnel soient déformées, endommagées ou que des tiers non autorisés y aient accès.
- que les systèmes installés peuvent être rétablis en cas d'interruption
- que les fonctions du système opèrent, que les erreurs de fonctionnement soient signalées (fiabilité) et que les données à caractère personnel conservées ne puissent pas être corrompues par un dysfonctionnement du système (intégrité). ;
- la définition d'un identifiant unique par utilisateur salarié du SI et interdit les comptes partagés entre plusieurs d'entre eux (même si quelques comptes partagés subsistent)
- que la recommandation de la CNIL concernant les mots de passe est respectée
- supprimer les permissions d'accès des utilisateurs dès qu'ils ne sont plus habilités à accéder à un local ou à une ressource informatique, ainsi qu'à la fin de leur contrat
- utiliser des logiciels régulièrement mis à jour
- Imposer l'utilisation d'un VPN pour l'accès au réseau local à distance (hors du lieu de travail)
- utiliser pour le réseau Wifi un chiffrement conforme à l'état de l'art (WPA 2, WPA2 PSK)

Tout ou partie des questions visant à évaluer le niveau de sécurité des données personnelles peuvent se trouver dans le guide de la CNIL – édition 2018 intitulé « sécurité des données personnelles ».

Sur ce point, le RGPD a créé l'exigence d'analyse d'impact (A) ainsi que l'obligation de notification des failles de sécurité (B) et contribue à une plus grande responsabilisation des sous-traitants vis-à-vis des responsables du traitement (C).

A. L'avènement de l'analyse d'impact

La contrepartie de cette liberté offerte par l'accountability tient au fait de mettre désormais à la charge du responsable du traitement ou du sous-traitant le soin de réaliser une analyse

d'impact que l'on peut définir comme une évaluation interne des risques d'atteinte à la vie privée des personnes concernées que certains traitements de données à caractère personnel peuvent faire encourir.

Il conviendra donc que les entreprises procèdent à un audit préalable afin de vérifier si elles sont susceptibles, compte tenu de leur activité, de la nature des données ou du traitement de données à caractère personnel envisagé, de faire courir un risque « élevé » d'atteinte à la vie privée des personnes concernées par ledit traitement et donc de déterminer si l'analyse d'impact doit ou non être réalisée.

B. L'obligation de notifier les violations de données personnelles

Jusqu'ici, seuls les fournisseurs de communication électronique avaient pour obligation de notifier à la CNIL (Commission Nationale de l'Informatique et des Libertés) les violations de données personnelles qu'ils avaient subies.

Le RGPD a le mérite de généraliser cette obligation de notification de violation de données personnelles, dans un délai de 72 heures à compter de la connaissance de cette violation, à l'autorité nationale de contrôle (CNIL en France), laquelle s'impose désormais à tout responsable de traitement ayant eu à subir une faille de sécurité, au sens d'une intrusion ayant entrainé la destruction, la perte, l'altération, ou l'accès non autorisé à des données personnelles, hormis quand il est en mesure de démontrer qu'il n'existe aucun risque pour les personnes (exemple : faille impliquant des données chiffrées et/ou anonymisées).

Par ailleurs, quand il existe un risque grave pour les personnes physiques concernées par la faille, le responsable du traitement se doit de les avertir personnellement de l'existence dudit risque, en plus des démarches initiées auprès de l'autorité nationale de contrôle.

Ladite notification devra d'ailleurs contenir :

- une description de la nature de la violation de données à caractère personnel y compris, si possible, les catégories et le nombre approximatif de personnes concernées par la violation et les catégories et le nombre approximatif d'enregistrements de données à caractère personnel concernés ;
- la communication du nom et des coordonnées du Délégué à la Protection des Données ou d'un autre point de contact auprès duquel des informations supplémentaires peuvent être obtenues ;
- une description des conséquences probables de la violation de données à caractère personnel ;
- une description des mesures prises ou que le responsable du traitement propose de prendre pour remédier à la violation de données à caractère personnel, y compris, le cas échéant, les mesures pour en atténuer les éventuelles conséquences négatives.

Une Politique de gestion des failles de sécurité devra être établie et devra prévoir l'investigation de la faille et l'apport des correctifs nécessaires. Le tout devra être documenté selon un process similaire aux éléments figurant ci-dessous.

A chaque fois qu'une faille de sécurité sera établie, une analyse devra être faite afin de déterminer si cette faille constitue ou non une violation de données personnelles au sens du RGPD.

Dans l'affirmative, l'entreprise déterminera s'il est nécessaire d'informer la CNIL, d'une part, et les personnes concernées, d'autre part.

Pour qu'il y ait violation, 2 conditions cumulatives doivent être réunies à savoir la mise en œuvre d'un traitement de données personnelles (1) et que ces données aient fait l'objet d'une violation (2) (perte de disponibilité, d'intégrité ou de confidentialité de données personnelles, de manière accidentelle ou illicite).

Dans le cadre de la procédure de gestion des failles de sécurité mise en place, il doit être prévu de documenter systématiquement en interne l'incident en déterminant :

- La nature de la violation si possible
- Les catégories et le nombre approximatif de personnes concernées par la violation les catégories et le nombre approximatif d'enregistrements de données à caractère personnel concernés

Il doit être prévu de décrire :

- Les conséquences probables de la violation de données ;
- Les mesures prises ou envisagées pour éviter que cet incident se reproduise ou atténuer les éventuelles conséquences négatives.

Si l'incident constitue un risque au regard de la vie privée des personnes concernées, il est notifié à la CNIL.

En cas de risque élevé, il est prévu d'informer également les personnes concernées. En cas de doute, il faudra le notifier à la CNIL qui déterminera ensuite s'il est nécessaire ou non d'informer les personnes.

La notification doit être transmise à la CNIL dans les meilleurs délais à la suite de la constatation d'une violation présentant un risque pour les droits et libertés des personnes.

En cas d'investigation, une notification en deux temps est possible :

- Une notification initiale dans les meilleurs délais à la suite de la constatation de la violation
- Puis, une notification complémentaire dans le délai de 72 heures si possible après la notification initiale. Si le délai de 72 heures est dépassé, il conviendra d'expliquer, lors de votre notification, les motifs du retard.

C. Une plus grande responsabilisation des sous-traitants vis-à-vis des responsables du traitement

Le RGPD consacre la possibilité d'un partage de responsabilités du traitement entre le responsable du traitement et le sous-traitant, mais précise surtout qu'il est attendu du responsable du traitement une obligation de vigilance quant au choix des sous-traitants.

On attend de lui qu'il s'assure que son sous-traitant présente des garanties de protection suffisantes dans le traitement des données personnelles.

Cela passera notamment par le fait de formaliser un contrat de sous-traitance dans lequel le sous-traitant attestera avoir mis en œuvre un certain nombre de mesures de sécurité élémentaires et en rapport direct avec la sensibilité et la quantité des données qu'il traite pour le compte du responsable du traitement et, principale innovation du RGPD, dans lequel seront décrites les obligations et les responsabilités inhérentes au responsable de traitement et au sous-traitant.

Nous sommes encore aujourd'hui dans l'attente des précisions de la Commission Européenne s'agissant du partage des obligations et des responsabilités et notamment de modèles types de clauses pour encadrer les responsabilités du responsable de traitement et du sous-traitant.

Le sous-traitant devra, par ailleurs, veiller à informer le responsable du traitement des failles qu'il aurait subies afin que le responsable du traitement puisse ensuite respecter l'obligation de notification à laquelle il est personnellement tenu.

III. La désignation obligatoire d'un Délégué à la Protection des Données (ci-après « DPD » - traduction française de Data Protection Officer ou « DPO »)

Parce que le principe d'accountability consiste en quelque sorte en un contrat de confiance entre l'autorité nationale de contrôle et les acteurs traitant de ces données que sont le responsable du traitement et son sous-traitant, le RGPD a voulu que certaines personnes, soit parce qu'elles sont une autorité publique ou un organisme public, soit parce qu'elles proposent un suivi régulier et systématique à grande échelle de données personnelles, soit parce qu'elles traitent des catégories particulières de données personnelles (parmi lesquelles les données sensibles), se voient dans l'obligation de désigner un DPD (ou DPO en anglais).

A l'instar du Correspondant Informatique et Libertés (CIL), le DPD peut être un salarié ou un intervenant extérieur de l'entreprise (avocat, consultant) à la condition qu'il présente des compétences juridiques suffisantes et que son indépendance soit garantie.

Ce délégué aura pour mission d'informer, de former et de conseiller le responsable du traitement ou le sous-traitant.
Il devra, par ailleurs, contrôler le respect du RGPD européen et de la loi nationale. Enfin, il coopérera avec l'autorité de contrôle et sera ainsi le point de contact de celle-ci.

Il est donc vivement conseillé à l'entreprise qui se verra dans l'obligation de désigner un DPD à compter du 25 mai 2018, de réfléchir, dès à présent, à la nomination d'un tel profil, qualifié d'abord de CIL et à terme DPD, afin que la mise en place de mesures visées dans le RGPD, au-delà même de sa simple nomination, soit envisagée et supervisée bien en amont de la date de mise en application du RGPD.

CONCLUSION

Ce tour d'horizon des avancées et des nouveautés issues du RGPD mérite que les sociétés s'y attardent et qu'elles se fassent conseiller dans la mise en œuvre des mesures qui seront attendues d'elles, eu égard aux risques accrus de sanctions (jusqu'à 4% du chiffre d'affaires annuel mondial total de l'exercice précédent ou 20 millions d'euros d'amende).

Il est donc essentiel qu'elles s'y préparent avec l'aide de leurs propres services juridiques, pour celles qui en ont les moyens, ou de prestataires extérieurs parmi lesquels les cabinets d'avocats intervenant en la matière.

Gageons que les moyens humains et financiers mis en œuvre ainsi que le temps qu'elles auront consacré en vue d'une mise en conformité complète de leurs systèmes d'information avec le RGPD seront autant d'éléments pris en compte par l'Autorité nationale de contrôle.

Une mise en conformité en bonne et due forme passe par :

- **un audit des pratiques du Client par recensement des informations ;**
- **l'élaboration d'un rapport d'audit identifiant les non conformités, d'une part, et faisant état des préconisations et des propositions d'actions, d'autre part ;**
- **une régularisation de ce qui d'un point de vue juridique peut l'être ce qui exclut de fait les prestations techniques qui seront sous-traitées à un tiers partenaire ou celui dont le Client fera savoir qu'il souhaite le solliciter pour ses compétences ou pour son expérience du système d'information du Client.**