LA REVUE DES JURISTES

DE SCIENCES PO

REVUE DE L'ASSOCIATION DES ÉLÈVES ET DIPLÔMÉS JURISTES DE SCIENCES PO • SEMESTRIEL • N° 10 • HIVER 2015

AJSP SciencesPo
ASSOCIATION DES JURISTES DE SCIENCES PO

L'éditorial du Comité de rédaction

Chers amis,

Ces deux dernières décennies, les innovations technologiques ont contribué à redessiner tant la nature que les modalités de nos échanges en créant, notamment, de nouveaux espaces de libertés : leur intégration au sein de cadres institutionnels constitue, par conséquent, un vaste défi.

La croissance de la branche du droit consacrée aux nouvelles technologies de l'information et de la communication (NTIC) est représentative de l'une des ambitions notables du droit positif qui consiste à suivre, accompagner – voire anticiper – les changements sociétaux : les problématiques qui en procèdent sont parmi les plus riches, complexes et intrinsèquement innovantes.

C'est dans une perspective désormais entérinée de transversalité que le Comité de rédaction de la *Revue des Juristes de Sciences Po* a lancé, en juillet dernier, un appel à contributions, sur le thème du Droit et des Nouvelles technologies qui recouvre l'ensemble des enjeux juridiques des technologies de l'information et de la communication, et leur impact sur le droit des affaires, le droit public, le droit pénal ou encore le droit international.

Semestriel à dimension « pratique » et « concrète », la Revue des Juristes n'en oublie pas moins ses objectifs scientifiques. La qualité du contenu des articles en témoigne. Afin de renforcer davantage sa richesse, l'innovation du numéro précédent, en la forme de la section « Points de vue », se voit consolidée et pérennisée. Celle-ci nous a permis d'inclure de nombreux entretiens qui donnent la mesure de la personnalité de certains acteurs du paysage juridique des NTIC, comme M^{e} Alain Bensoussan. Du « *cloud* » à l'Impression 3D, en passant par le *Big Data*, tant de termes barbares, quoiqu'éminemment actuels, qui sont envisagés ici par l'impitoyable rigueur du prisme juridique.

Nous tenons à remercier tous nos contributeurs, acteurs de la réussite de la Revue des Juristes de Sciences Po. Nous nous attachons en outre à souligner l'apport précieux de notre Directeur scientifique Jean-Baptiste Soufron, ancien avocat et secrétaire général du Conseil National du Numérique. La pertinence et la justesse de ses nombreux conseils et commentaires nous ont été d'une grande utilité tout au long de la construction de ce numéro.

Enfin, alors que ces numéros semestriels constituent la « matière première » de notre travail, la pérennité de notre démarche passe aussi par des projets de plus long-terme. A cet effet, nous sommes heureux et honorés de pouvoir annoncer le lancement d'un

partenariat avec l'éditeur LexisNexis, effectif depuis la fin de l'année 2014. Nous sommes ainsi la première revue juridique étudiante à être référencée sur leur base de données en ligne. Cela nous a permis d'accroître la visibilité de notre travail et de celui de nos contributeurs présents et futurs. Dans une perspective toujours transversale, notre prochain numéro d'été 2015 portera sur le Droit et la Violence. Un Appel à contributions sur cette thématique se trouve en fin du présent numéro. En attendant, nous vous souhaitons, chers amis de la RJSP, juristes ou non, une excellente lecture.

Le Comité de rédaction

Gwennhaëlle Barral
M2 Droit économique, spécialité Contentieux économique et arbitrage
Rédactrice en chef

Victor Charpiat
M2 Droit économique, spécialité Entreprises, marchés, régulations
Responsable de la publication

Thomas Chanzy
M2 Droit économique, spécialité Global Business Law and Governance

Marin Denizet
M2 Droit économique, spécialité Entreprises, marchés, régulations

Alexandra Husson
M2 Carrières judiciaires et juridiques

Flore Mevel
M2 Carrières judiciaires et juridiques

Laura Montagnier
M2 Droit économique, spécialité Entreprises, marchés, régulations

Anaïs Aubert
M1 Droit économique

Ambroise Fahrner
M1 Droit économique

Ernst-Wesley Laîné
M1 Droit économique

Carolin Stenz
M1 Droit économique

François Weidler-Bauchez
M1 Droit économique

Sommaire

POINTS DE VUE

ENTRETIEN AVEC Me ALAIN BENSOUSSAN

Le droit de la robotique : aux confins du droit des biens et du droit des personnes

« Une démarche éthique est indispensable dans la construction d'un droit de la robotique »

ALAIN BENSOUSSAN

Avocat associé, Lexing Alain Bensoussan Avocats

Avocat au barreau de Paris depuis 1978, Me Alain Bensoussan est le fondateur du cabinet Alain Bensoussan Avocats, désormais intégré dans le réseau international Lexing, le premier réseau de cabinets d'avocats spécialisés dans le droit des technologies avancées. Après avoir exploré le droit de l'informatique, le droit des télécoms et le droit de l'Internet, Me Alain Bensoussan[1] travaille désormais sur le droit des robots[2], thème de l'entretien qu'il a accordé à la Revue des juristes de Sciences Po.

***La Revue des juristes de Sciences Po[3] :* Votre spécialisation dans le droit de l'informatique a été très précoce. Comment vous est venu cet intérêt pour l'informatique ?**

Me Alain Bensoussan : J'ai d'abord étudié le droit et l'économie, à Sciences Po et à Dauphine. A cette époque, l'informatique commençait à se développer. Il y avait un atelier de COBOL à Sciences Po (*ndlr : le COBOL est un langage de programmation*) et c'est dans ce cadre-là que je me suis passionné pour l'informatique. Je suis toujours resté des deux côtés : j'ai appris à programmer et j'ai voulu participer à l'élaboration d'un droit de l'informatique, qui, à l'époque, se limitait à la loi Informatique et Libertés[4]. En 1985, année de la loi qui a permis aux

[1] Depuis janvier 2013, il assure une chronique juridique dans le magazine Planète Robots et est l'auteur d'une « *charte sur les droits et devoirs des robots* » disponible sur http://www.alain-bensoussan.com/wp-content/uploads/2014/09/24091796.pdf.

[2] Informations disponibles sur : http://www.alain-bensoussan.com/avocat-robot-et-droit/.

[3] Propos recueillis par Victor Charpiat et François Weidler-Bauchez, pour la Revue des juristes de SciencesPo.

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

logiciels d'être protégés par le droit d'auteur[5], j'ai publié le premier Traité sur le droit de l'informatique[6]. Je n'ai jamais quitté le droit de l'informatique, mais j'ai ensuite travaillé sur le droit des télécoms, puis sur le droit de l'Internet, et maintenant sur le droit des robots.

Comment ces droits « des nouvelles technologies » se développent-ils ? Se développent-ils à partir d'un tronc commun ?

Le point commun à toutes ces nouvelles branches du droit, c'est le droit du numérique. Tous ces secteurs exploitent une ressource nouvelle : la donnée.

La donnée possède trois propriétés :

- son coût de reproduction est quasi nul, ce qui induit un changement de paradigme économique ;

- elle est indéfiniment appropriable : la donnée peut être effectivement partagée par plusieurs acteurs, alors que, dans le champ du droit patrimonial, la copropriété reste une fiction juridique ;

- elle est devenue transversale ; presque tous les secteurs de l'économie trouvent leurs vecteurs de croissance dans l'utilisation de la donnée : le bâtiment, la voiture, et même des objets du quotidien, comme la table, deviennent intelligents.

Dans ce sens, le numérique est transversal et structure les droits des nouvelles technologies.

Vous avez développé le concept de « personnalité robot ». Si les robots méritent de former une catégorie juridique à part entière, c'est donc qu'ils sont distincts des biens traditionnels.

Le droit des biens est un droit « statique ». C'est un droit conçu pour des objets inanimés. Or, même si les robots ne deviendront jamais des humains à part entière, ils les dépasseront sur de nombreux points. C'est en tout cas l'opinion de personnalités apparentées au courant transhumaniste, comme Ray Kurzweil, qui est maintenant l'un des responsables de la technologie chez Google, Chris Anderson, l'ancien rédacteur en chef de Wired, ou Nicholas Negroponte, professeur au Massachussetts Institute of Technology. L'estimation la plus couramment retenue de la date du basculement vers la « *singularité* », c'est-à-dire du dépassement des capacités de l'intelligence humaine par l'intelligence artificielle, est 2035[7]. Cela semble irréaliste, mais l'intelligence artificielle progresse à une vitesse incroyable : en 1997, un ordinateur a vaincu le champion du monde d'échecs, Garry Kasparov ; en 2011, le programme Watson a battu les champions du jeu Jeopardy! (*ndlr : Jeopardy! est un jeu télévisé où les candidats doivent retrouver une question à partir des réponses*) ; en 2014, un ordinateur a réussi le test de Turing (*ndlr : le test de Turing consiste à organiser une conversation* « aveugle » *entre un ordinateur et un examinateur : si l'examinateur n'est pas capable de distinguer lequel*

[5] Loi n° 85-660 du 3 juillet 1985 relative aux droits d'auteur et aux droits des artistes-interprètes, des producteurs de phonogrammes et de vidéogrammes et des entreprises de communication audiovisuelle, titre V « Des logiciels ».
[6] A. BENSOUSSAN, *Droit de l'informatique et de la télématique,* Éditions Berger-Levrault, 1985.
[7] A. VON SCHWANGAU, « *Le monde en 2035 - le début d'un nouveau paradigme* », Horizon2050, 18 octobre 2012.

de ses interlocuteurs est un ordinateur, le test est réussi). Dans ce contexte, la décision de Barack Obama, d'encourager l'apprentissage de la programmation dès le plus jeune âge, est très responsable.

Les robots vont devenir meilleurs que les humains dans l'exécution de tâches qui demandent une capacité d'analyse de l'environnement. Ce n'est pas tant l'intelligence artificielle qui permet ce basculement que le perfectionnement des capteurs : les robots entendent, voient, sentent bien mieux que nous. Et comme les informations traitées par les capteurs peuvent être croisées avec les données qui existent déjà – par le biais d'Internet ou du Big Data – les robots vont développer une capacité d'analyse gigantesque.

Mais pourront-ils remplacer les avocats ?

Les robots savent déjà écrire des articles sur les résultats sportifs ou l'évolution de la bourse. Des questions très directes se posent déjà : doit-on indiquer que l'article a été écrit par un robot ? Un humain peut-il signer l'article écrit par un robot ? Le métier d'avocat sera aussi robotisé, dans une certaine mesure. Certes, le cœur de l'activité de l'avocat restera longtemps assuré par des humains, mais les robots permettront d'automatiser des tâches laborieuses. Par exemple, un robot pourrait très bien constituer le dossier thématique préalable à la rédaction d'un article. Il pourrait même le faire mieux qu'un humain, car il comprendrait toutes les langues.

Quels seraient donc les attributs de la « personnalité robot » ?

Il faut comprendre la personnalité robot comme un nouveau genre : dans les registres de la sécurité sociale, on utilise le 1 pour les hommes et le 2 pour les femmes. Alors, il faudrait utiliser le 3 pour les robots !

En fait, la vocation d'un robot est de fonctionner de manière autonome dans un environnement fermé ou ouvert, en coopération avec l'Homme. Si le robot évolue dans un environnement ouvert, il peut interagir avec n'importe qui. Il est donc indispensable que le robot soit reconnaissable : il lui faut un numéro d'immatriculation, un nom et un capital, un peu comme pour une personne morale. Car si le robot cause un dommage, il faut prévoir les recours contre lui.

Dans la loi du Nevada, qui, je l'espère, servira de modèle, le robot est doté des principaux attributs de la personne morale, même s'il n'est pas explicitement qualifié ainsi. Il dispose d'un numéro et d'une assurance, et il est répertorié dans un fichier.

Comment peut-on régler le problème de la responsabilité du robot ?

Sur cette question, les américains ont opté pour une approche pragmatique. La responsabilité du robot ne constituerait pas un bloc, mais serait partagée par les différents intervenants, eux-mêmes hiérarchisés : c'est la responsabilité en cascade. En premier lieu, le concepteur de l'intelligence artificielle du robot serait responsable. Ensuite, seulement, la responsabilité du fabricant du robot ou de son propriétaire ou utilisateur pourrait être recherchée.

Il s'avère que le livre vert publié par la Commission européenne penche plutôt pour une reconnaissance de la responsabilité du propriétaire du robot. Dans le cadre de la robotique, je ne suis pas favorable à une utilisation trop étendue du concept de propriété. L'utilisateur du robot me semble avoir plus de responsabilité que le propriétaire, car le robot et son utilisateur interagissent, et cette interaction peut déboucher sur une modification du comportement du robot. La plupart des robots sont auto-apprenants : si, dans une certaine mesure, il est possible de les « éduquer », la responsabilité de l'utilisateur devrait primer sur celle du propriétaire.

Quel est le lien entre la responsabilité du robot et le fait de lui attribuer un capital ?

Idéalement, plus le robot serait exposé à des risques, plus le capital rattaché à sa personne devrait être élevé. Ce capital pourrait être assorti d'une garantie bancaire. On peut également imaginer la création d'un fonds de garantie qui serait alimenté par un prélèvement sur les primes d'assurance, comme en matière d'indemnisation des victimes d'accidents de la circulation.

L'attribution d'un capital au robot devrait aller de pair avec une obligation d'assurance. C'est sous cet angle que les américains abordent le problème des voitures intelligentes. Pour qu'une voiture sans conducteur puisse rouler dans l'État de Californie, il faut qu'elle soit assurée à hauteur de 5 millions de dollars[8]. Il faut donc constituer des fichiers pour répertorier les voitures intelligentes, afin de s'assurer que chaque voiture qui roule est assurée : d'où la nécessité d'un « numéro d'identité ».

En l'attente d'une réforme d'envergure, comment le robot entre-t-il dans le système juridique ?

Les robots ont déjà pénétré dans nos vies quotidiennes. Il est temps de les intégrer à d'autres catégories de normes : loi Informatique et Libertés, respect de la dignité des robots, secret industriel, application de la loi sur la fraude informatique[9] pour sanctionner les piratages de robots – il faudrait d'ailleurs envisager des circonstances aggravantes, car un robot piraté peut être beaucoup plus dangereux qu'un ordinateur.

Quant à la théorie de la personnalité robot, elle entre dans le système juridique, tout simplement car elle structure les contrats des professionnels que nous conseillons. Or le contrat tient lieu de loi entre les parties, et, lorsqu'un juge est amené à régler un litige, il se réfère aux stipulations contractuelles.

Quel rôle peut jouer l'éthique dans l'élaboration du droit des robots ?

Avoir une démarche éthique est indispensable dans la construction d'un droit de la robotique, car la règle éthique et la règle juridique s'imbriquent inévitablement. Imaginez qu'une voiture sans pilote s'apprête à percuter une personne âgée qui traverse la route, tout en étant suivie de près par une voiture transportant des enfants qui ne sont pas attachés. Si la voiture sans pilote freine, elle évite la personne âgée, mais les enfants risquent d'être projetés en avant par le freinage. Alors quel critère doit être prépondérant dans la prise de décision de la voiture

[8] État de Californie, Senate Bill No. 1298, Chapter 570, Section 2.
[9] Loi n° 88-19 du 5 janvier 1988 relative à la fraude informatique, désormais codifiée dans le Code pénal aux articles 323-1 et suivants.

intelligente confrontée à une situation de ce type, où il faut choisir entre deux dommages ? L'intérêt de la société ? Le débat est ouvert, mais il sera indispensable de définir des règles du jeu qui prendront en compte le fait que l'humain et le robot n'ont pas les mêmes capacités de calcul.

ENTRETIEN AVEC Me CHARLES-HENRI BOERINGER

État des lieux des visites inopinées, perquisitions et gardes à vue dans l'entreprise : l'enjeu de la saisie des données

« Les nouvelles technologies rendent les sociétés plus vulnérables face aux enquêtes »

CHARLES-HENRI BOERINGER

Avocat *counsel*, Clifford Chance, Paris

Diplômé de l'Institut d'études politiques de Paris et de l'Université Paris II Panthéon-Assas, ancien Secrétaire de la Conférence des avocats du barreau de Paris, Charles-Henri Boeringer est avocat counsel chez Clifford Chance, spécialisé en contentieux commercial et en droit pénal des affaires. Il est le coauteur, avec Thomas Baudesson et Karine Huberfeld, du Guide pratique des visites inopinées, perquisitions et gardes à vue dans l'entreprise[1]*, dont la seconde édition est parue en juillet 2014.*

***La Revue des Juristes de Sciences Po*[2] : La réédition de votre ouvrage s'inscrit-elle dans un contexte particulièrement sensible ? Pouvez-vous nous indiquer les évolutions notables depuis 2007 (date de l'édition précédente) et leur lien éventuel avec les nouvelles technologies ?**

Me Charles-Henri Boeringer : Plusieurs éléments justifient cette nouvelle édition. D'abord, l'augmentation constante du nombre d'autorités dotées de pouvoirs d'enquête et de contrôle (par exemple, le Défenseur des droits ou l'Agence nationale de sécurité du médicament, se sont récemment ajoutés à bien d'autres administrations et autorités administratives indépendantes). En outre, les sociétés sont de plus en plus soumises à des procédures de vérification et, le cas échéant, de sanction, visant à s'assurer de leur « conformité ». Le risque pour une société d'être confrontée à une visite inopinée est devenu presque normal – et non plus exceptionnel.

[1] T. BAUDESSON, C.-H. BOERINGER, K. HUBERFELD, *Guide pratique des visites inopinées, perquisitions et gardes à vue dans l'entreprise,* 2e édition, Lexisnexis, 2014.

[2] Propos recueillis par Gwennhaëlle Barral et Victor Charpiat, pour la Revue des Juristes de Sciences Po.

Soulignons aussi que les nouvelles technologies rendent plus vulnérables les sociétés face aux enquêtes. Lorsqu'un régulateur se présente dans une entreprise dans le but d'effectuer une visite inopinée, il exige, en général, la présence du directeur informatique pour obtenir les accès aux données. De nombreux débats ont lieu depuis quelques années concernant les saisies massives de données informatiques par certains enquêteurs et la jurisprudence commence à apporter des réponses.

D'un point de vue strictement juridique, depuis 2007, une série de décisions et d'interventions législatives et réglementaires – le fameux arrêt Ravon, notamment – a permis de réglementer les visites inopinées en prévoyant la possibilité de recours et un certain renforcement des droits de la défense. La jurisprudence a été à l'origine d'une certaine remise en ordre de procédures qui n'étaient pas suffisamment encadrées et laissaient sans doute le champ trop libre aux enquêteurs. Il est par exemple devenu obligatoire, dans beaucoup de procédures de visite inopinée, que les enquêteurs notifient à la personne concernée la faculté de se faire assister par un avocat. La CEDH vient aussi de condamner la République Tchèque dont le droit – comme le droit français – n'offre pas la possibilité d'un contrôle juridictionnel effectif *a posteriori* de la nécessité de la mesure simple (ou sur pouvoir propre) opérée par leur régulateur en matière de concurrence. Cet encadrement accru entraîne par ailleurs une complexification de la matière rendant très utile ce guide pratique.

Quelles sont les différentes catégories de visite inopinée ?

Il existe trois grandes catégories de visites inopinées : la visite pénale, la visite administrative et la visite intervenant dans le cadre d'un litige civil ou commercial (fondée sur l'article 145 du Code de procédure civile).

Si l'on met à part la visite de l'article 145 – qui n'est jamais coercitive – une *summa divisio* est commune aux visites pénales et administratives. Soit la visite est autorisée par un magistrat du siège (le juge d'instruction ou le juge des libertés et de la détention) et dans ce cas, elle est coercitive et laisse un large pouvoir aux enquêteurs ; soit elle ne l'est pas, et dans ce cas les enquêteurs ont des pouvoirs plus limités.

Au-delà de cette grande distinction, il existe autant de régimes différents que d'autorités habilitées à mener des visites inopinées. Les enquêteurs des douanes, n'ont pas les mêmes pouvoirs que ceux de la CNIL ou de l'ANSM. Il est donc difficile de s'y retrouver, même s'il me semble que les régimes ont tendance à converger.

Dans quelles situations est-il possible de refuser de fournir certaines informations ?

Tout dépend du cadre juridique dans lequel intervient la visite inopinée. En dehors du cadre coercitif, c'est-à-dire, autorisé par un magistrat du siège, la société a plus de marge de manœuvre pour refuser de fournir certaines informations.

En présence d'une ordonnance du juge (généralement le juge des libertés et de la détention), la société doit fournir tous les documents qui lui sont demandés, à deux exceptions près :

- la documentation couverte par le secret professionnel entre l'avocat et son client, quel que soit la nature ou le contenu des correspondances ;

- la documentation couverte par le secret-défense : la société n'a pas le droit de fournir des informations couvertes par le secret-défense, sauf celui-ci a été préalablement levé ;

Les enquêteurs sont aussi soumis aux principes de spécialité et de proportionnalité : ils ne peuvent pas saisir tous les documents qu'ils trouvent ; ils doivent, en principe, se limiter aux documents ayant un lien avec leur enquête.

En pratique, certains enquêteurs ont tendance à vouloir saisir l'intégralité d'une boite email ou d'un disque dur. Ce faisant, ils risquent de saisir des messages couverts par le secret professionnel ou des messages n'ayant aucun rapport avec l'enquête. Il convient dans ce cas d'exiger des enquêteurs qu'ils extraient préalablement les documents couverts par le secret professionnel de la masse des documents saisis. En cas de refus, il faut le faire acter au procès-verbal établi en fin de visite.

Les visites domiciliaires constituent-elles une menace pour le rapport privilégié entre l'avocat et son client ?

Il faut souligner une évolution positive : la jurisprudence a mis de l'ordre dans la pratique qui consistait, pour l'autorité effectuant la visite domiciliaire, à emporter tous les documents qu'elle trouvait, pour ensuite les trier dans un second temps. Cette pratique permettait par exemple à l'autorité en question de prendre connaissance des messages échangés entre l'avocat et son client. Elle n'avait, certes, pas le droit de les exploiter ou de les mettre au dossier, mais le seul fait de les lire peut être de nature à renforcer la démarche de l'autorité. Les avocats ont vigoureusement protesté contre cette pratique. Ils ont défendu le caractère secret de ces correspondances. L'autorité ne doit pas seulement s'abstenir de les exploiter : elle ne doit tout simplement pas y toucher.

Après avoir été assez laxiste, la jurisprudence semble aujourd'hui consacrer le fait que la violation du secret professionnel intervient dès la saisie des données concernées, de sorte qu'une extraction postérieure, par l'autorité, des pièces couvertes par le secret professionnel, ne paraît plus admissible. Mais la question de la sanction reste encore en suspend. S'agit-il de la nullité de l'opération de visite et de saisie dans son intégralité, ou simplement du retrait du dossier des pièces couvertes par le secret professionnel ? Cela reste à trancher. Selon moi, seule la première option est de nature à protéger efficacement les droits de la défense.

Comment fait l'autorité quand elle se retrouve face à des données cryptées ou protégées par des mots de passe ?

De la même manière qu'il est interdit de faire entrave à une visite domiciliaire, en empêchant les inspecteurs de pénétrer dans les locaux, il est aussi interdit de l'entraver en les empêchant d'accéder au contenu des ordinateurs. L'autorité d'enquête a donc le droit d'exiger les mots de passe permettant d'accéder aux données informatiques protégées. Tous les mots de passe sont concernés : ceux qui permettent d'accéder à une session, ceux qui permettent d'accéder aux données stockées en ligne dans un service de *cloud computing*, et ceux qui protègent des fichiers particuliers à l'intérieur des sessions.

Toutefois, les données ou documents doivent appartenir à l'entreprise, et non personnellement aux salariés. Les correspondances personnelles qui transitent par les messageries professionnelles peuvent être saisies. Mais les messageries personnelles des salariés ne sont pas concernées, à moins d'être explicitement visées par l'ordonnance.

Dans ce cadre, quels sont les enjeux du *bring your own device* (BYOD) (le fait qu'un nombre croissant de salariés utilise son matériel informatique personnel pour un cadre professionnel) ?

Le critère est l'appartenance ou non à l'entreprise du matériel. Si l'ordinateur appartient manifestement au salarié, il n'est pas possible pour l'autorité d'enquête d'y accéder, sauf si l'ordonnance le prévoit expressément. L'autorité qui requiert l'ordonnance peut notamment prévoit cette possibilité lorsqu'elle sait que les salariés de l'entreprise ont l'habitude de travailler depuis leur domicile et/ou sur leur matériel personnel.

Quel type de différences existe-t-il entre notre système juridique et les systèmes de *common law* quant aux visites domiciliaires ?

La différence fondamentale tient dans l'existence du *legal privilege*.

Il existe deux différences entre le *legal privilege* et le secret professionnel.

D'abord, le secret professionnel n'est défini, en France, qu'en rapport avec l'identité du destinataire ou du récepteur de la correspondance. Seules les correspondances avec un avocat sont couvertes par le secret professionnel. Par exemple, les communications internes entre le directeur juridique et ses collaborateurs peuvent porter sur le même sujet que les correspondances avec l'avocat, mais elles ne sont pas concernées par le secret professionnel, quand bien même le directeur juridique aurait par ailleurs la qualité d'avocat.

Au contraire, dans les systèmes de *common law*, le *legal privilege* protège également les correspondances du *in-house lawyer*. En France, pour bénéficier du secret professionnel, il faut non seulement être inscrit à un barreau mais aussi exercer professionnellement comme avocat. Aux États-Unis, le fait d'être inscrit à un barreau suffit, même si l'avocat est salarié.

Ensuite, contrairement au secret professionnel, le *legal privilege* prend également en compte la nature et le contenu du message. Les correspondances du directeur juridique et de ses collaborateurs ne sont donc pas toutes protégées par le *legal privilege*. Le *legal privilege* est donc un système plus complexe que le secret professionnel, mais aussi plus protecteur.

LOÏC JOURDAIN, MICHEL LECLERC & ARTHUR MILLERAND

Les enjeux juridiques des modèles économiques de consommation collaborative

LOÏC JOURDAIN, avocat et autoentrepreneur

MICHEL LECLERC, avocat, Freshfields Bruckhaus Deringer LLP, Paris

ARTHUR MILLERAND, avocat, Clifford Chance, Paris

RÉSUMÉ

Depuis quelques années, les acteurs économiques traditionnels sont concurrencés par de nouveaux acteurs qui maîtrisent la technologie, Internet et, par ce biais, les informations disponibles. Ceux-ci fédèrent de très nombreux utilisateurs et forment de réelles communautés dont l'importance économique est grandissante. Seulement, leur croissance est plus rapide que l'adaptation et l'appréhension de ces nouvelles pratiques par le droit, ce qui crée une certaine insécurité juridique. Tel est le constat qui nous a conduit à lancer le blog « Droit du Partage » (www.droitdupartage.com ; @droitdupartage sur Twitter ; droitdupartage@gmail.com).

On n'entend plus que parler d'eux, ou presque – Uber, Blablacar, Tripadvisor, Airbnb, Couchsurfing, Ulule sont autant d'exemples qui viennent offrir aux consommateurs une alternative aux schémas de consommation classiques. Leurs modèles économiques reposent tous sur une constante, quel que soit leur secteur d'activité : l'optimisation de la disponibilité de biens, d'informations et de compétences, pour les partager et en faire profiter tous les utilisateurs. Quant à leur philosophie, elle repose systématiquement sur la monétisation d'un actif inutilisé, à temps plein ou partiel, ou la mise en commun de ce qui existe pour en faire bénéficier offreurs et demandeurs du service respectif.

Toutes ces entreprises se reposent sur des plateformes Internet, garantes de la confiance nécessaire à la mise en relation des utilisateurs, pour que les biens ou les services s'échangent à moindre coût. Cette intermédiation permet dans le même temps, grâce aux données qui transitent par leur biais, d'offrir une plus grande personnalisation. Le développement de cette nouvelle façon de consommer et de produire entraîne une mutation économique profonde. Celle-ci est porteuse de nouveaux problèmes/questions juridiques auxquelles le blog « Droit

du Partage » se confronte, chaque jour, pour apporter des décryptages et des réponses juridiques.

Grâce aux données qui transitent par leur biais, cette intermédiation permet dans le même temps d'offrir une plus grande personnalisation. Cette nouvelle façon de consommer et de produire entraîne une mutation économique profonde, qui est porteuse de nouveaux problèmes/questions juridiques. Le blog « Droit du Partage » s'y confronte, chaque jour, pour apporter des décryptages et des réponses juridiques.

Une mutation économique profonde

La naissance et l'expansion de cette économie collaborative est porteuse d'une mutation économique profonde, qui modifient l'équilibre des secteurs traditionnels en introduisant une nouvelle façon de consommer. Cette « *économie du partage* » se diffuse et touche tous les domaines sans distinction.

Qu'il s'agisse du secteur des transports où des utilisateurs peuvent se déplacer en covoiturage en milieu urbain (UberPop) ou sur de longues distances (Blablacar), de la restauration avec la possibilité de se nourrir chez son voisin (Cooknshare), de l'hôtellerie où chacun peut louer un appartement dans une ville pour quelques jours à prix moindre (Airbnb), ou encore du développement des monnaies virtuelles qui conduit à se dispenser d'avoir recours à une monnaie « physique » (paiement par mobile ou Bitcoin), ces nouveaux auxiliaires se diffusent et prospèrent.

Leur succès est fulgurant pour au moins trois raisons : (i) l'offre proposée est presque infinie, (ii) les intermédiaires sont supprimés et (iii) les valeurs d'altruisme (partage, convivialité, échange, confiance) sont mises en avant. De plus, ces acteurs permettent d'offrir une expérience client optimisée, puisque la technologie conduit à fournir un service généralement géolocalisé et à moindres coûts. Enfin, certaines entreprises se servent de cette maîtrise technologique pour mettre en relation les utilisateurs sur leur plateforme en temps réel. Ces réseaux *peer-to-peer* (« P2P »), à l'ergonomie travaillée, rendent possible la rencontre d'une offre et d'une demande entre particuliers qui partagent les mêmes intérêts.

Ainsi, les propositions commerciales de ces nouveaux acteurs paraissent mieux adaptées que celles des acteurs « traditionnels », ce qui les conduit à gagner des parts de marché à une très grande vitesse et à fidéliser leurs utilisateurs.

Les chiffres sont à cet égard éloquents :

- en 2013 le marché mondial de l'économie collaborative est estimé à 3,5 milliards de dollars[1] ;

- à terme le marché mondial devrait représenter 110 milliards de dollars[2].

[1] Cf. Commission européenne, « *Business Innovation Observatory: The Sharing Economy. Accessibility Based Business Models for Peer-to-Peer Markets* », 2013. http://ec.europa.eu/enterprise/policies/innovation/policy/business-innovation-observatory/files/case-studies/12-she-accessibility-based-business-models-for-peer-to-peer-markets_en.pdf.

A titre d'exemple, aujourd'hui, l'offre d'hébergement Airbnb à Paris est équivalente à l'offre d'hôtels 3 étoiles, représentant environ 30 000 logements, ce qui en fait une concurrence considérable pour le secteur hôtelier.

Outre les performances économiques de cette nouvelle économie, ce phénomène impressionne par les profonds changements sociaux qu'il entraine. L'usage prend ainsi le pas sur la propriété et l'« *âge de l'accès* », par opposition à celui de l'avoir, décrit par Jeremy Rifkin[3], semble se concrétiser. Dans son dernier livre[4], Rifkin va jusqu'à prédire la fin de la société de consommation capitaliste grâce à l'émergence de ces nouvelles communautés collaboratives.

Néanmoins, il faut garder à l'esprit que ces acteurs de l'économie collaborative ne se développent pas par pur altruisme. Leur développement repose sur l'affinité de ces plateformes avec les réseaux sociaux, et ils s'appuient sur une utilisation performante des données de masse (« *Big Data* »). Ce faisant, ils n'oublient pas de se rémunérer, et ces nouveaux modèles économiques, s'ils reposent sur une philosophie du partage, n'en sont pas moins capitalistes. Ainsi, ces acteurs sont en voie de devenir des superpuissances économiques.

Se pose donc naturellement la question de l'encadrement juridique de ces nouveaux modèles économiques auxquels des millions de français ont d'ores et déjà recours quotidiennement.

Problèmes juridiques sous-jacents

Aucune des utilisations de ces nouvelles plateformes de l'économie collaborative n'est juridiquement neutre. Les interrogations ne manquent pas : qui ne s'est jamais demandé s'il avait réellement le droit de sous-louer son appartement sur Airbnb ? Qui ne s'est jamais demandé s'il était assuré en cas d'accident de la circulation en utilisant Uber ou Blablacar ? Qui ne s'est jamais interrogé sur le sort de ses données personnelles en créant un compte pour utiliser un site Internet ? Quels sont les droits et garanties du sous-acquéreur d'un bien d'occasion ?

Le droit est omniprésent tant pour ces nouveaux acteurs économiques, que pour les utilisateurs de ces plateformes de mise en relation. Aussi, de nouvelles problématiques juridiques émergent dans différentes situations :

- **le contentieux avec les acteurs traditionnels** : les nouveaux acteurs viennent directement concurrencer les acteurs traditionnels de certains secteurs, ce qui conduit à des crispations. L'entrée sur le marché de ces nouvelles entreprises vient remettre en question des situations que l'on pensait acquises. C'est ainsi que les taxis ont fortement

---

[2] J. CONTRERAS, « *MIT Sloan grad on the "sharing economy", the next big trend in social commerce* », déc. 2011. http://mitsloanexperts.mit.edu/mit-sloan-grad-on-the-sharing-economy-the-next-big-trend-in-social-commerce/.

[3] J. RIFKIN, «*The Age of Access* », J.P. Tarcher/Putnam, 2000.

[4] J. RIFKIN, «*La nouvelle société du coût marginal zéro. L'Internet des objets, l'émergence des communaux collaboratifs et l'éclipse du capitalisme* », Ed. Les Liens qui libèrent, 2014.

réagi contre les véhicules de tourisme avec chauffeur (VTC)[5], ou encore que le secteur hôtelier se mobilise contre Airbnb et les particuliers qui offrent leurs logements à une location de courte durée[6]. Ces joutes juridiques soulèvent notamment des questions de concurrence déloyale et de pratiques commerciales trompeuses ;

- **l'adaptation législative et réglementaire de certains secteurs** : les règles existantes ne sont parfois pas adaptées aux schémas économiques de ces nouveaux acteurs. Si la France se targue d'avoir le meilleur régime au monde pour le crowdfunding depuis l'adoption d'une ordonnance en la matière[7], dans d'autres domaines il n'existe tout simplement pas encore de cadre juridique (les monnaies virtuelles avec le phénomène Bitcoin[8] par exemple). L'inadaptation des règles juridiques conduit à créer une insécurité juridique, à la fois pour les entreprises et pour les utilisateurs ;

- **les interrogations des entrepreneurs** : les nouveaux acteurs de l'économie collaborative se retrouvent confrontés à des problématiques juridiques nouvelles, et souvent non précisément appréhendées par le droit. Il est donc nécessaire de procéder à une analyse des règles existantes afin de rendre possible le déploiement de leur *business* (par exemple, l'obtention d'un agrément auprès de l'Autorité des Marchés Financiers (AMF) ou de l'Autorité de contrôle prudentiel et de résolution (ACPR) dans le cas du crowdfunding). A tout le moins, le conseil juridique doit fournir une analyse des risques pour anticiper les contentieux et les problématiques règlementaires (par exemple, la Direction générale de la concurrence, de la consommation et de la répression des fraudes (DGCCRF) ou la Commission nationale de l'informatique et des libertés (CNIL)) De ce fait, l'accompagnement des entrepreneurs dans ces nouveaux domaines s'avère souvent difficile mais essentiel, ce qui nécessite l'intervention d'un avocat spécialisé ;

- **les risques encourus par les utilisateurs** : les utilisateurs, qui ont recours à ces outils par simplicité, par goût, ou simplement pour faire des économies, sont souvent, sans le savoir, en risque juridique. C'est ainsi que chacun doit être attentif aux conséquences de l'utilisation de ces services. Pour ses données personnelles (par exemple, le métier d'Uber n'est pas seulement le transport mais aussi l'information qui permet de fournir un service personnalisé et gérer au mieux sa flotte de véhicule) ; pour sa situation fiscale (par exemple, lorsque des bénéfices sont réalisés en vendant des Bitcoin il faut utiliser le bon régime fiscal), pour sa situation sociale (par exemple, les locations à courte durée peuvent poser des problèmes de travail dissimulé), ou encore pour sa situation personnelle (par exemple, la sous-location de son logement grâce à Airbnb).

De manière générale, tous les acteurs de cette économie collaborative doivent être vigilants et accompagnés par des spécialistes pour déterminer ce qui est juridiquement possible, pour pouvoir identifier les risques (et les réduire le cas échéant) et y faire face en cas de réalisation du risque (par exemple, en présence d'un litige ou d'un contrôle par une autorité de règlementation).

[5] Voir les récentes décisions rendues à l'encontre d'Uber et Uberpop.
[6] Des actions en justices sont régulièrement initiées dans ce cadre.
[7] Ordonnance n° 2014-559 du 30 mai 2014 relative au financement participatif.
[8] Des projets de régulation du Bitcoin sont en cours d'étude, notamment aux Etats-Unis et en France.

Notre blog « Droit du partage » : la diffusion des analyses juridiques

Face à ce constat, nous avons décidé de mettre à profit notre expérience accumulée en accompagnant des clients, des jeunes entreprises, mais aussi des amis, dans leurs projets entrepreneuriaux ou dans leur vie quotidienne, et de la partager, pour que la connaissance juridique des enjeux liés à l'utilisation de l'économie collaborative se diffuse.

Le phénomène de consommation collaborative modifie le contexte dans lequel le droit est amené à s'appliquer. Il paraît donc indispensable d'échanger dès à présent ensemble sur ces nouvelles modalités.

C'est dans cette perspective que notre blog « Droit du Partage » adopte une démarche triple :

- **Comprendre** : ces phénomènes étant nouveau, aucune réponse ne se trouve uniquement dans les manuels traditionnels ou les moteurs de recherches juridiques utilisés classiquement. Comprendre les nouvelles tendances suppose donc une exploration autonome des auteurs de ce blog par une approche pluridisciplinaire du droit ;

- **Faire comprendre** : il ne s'agit pas ici d'entrer dans un dialogue entre experts qui ne se liraient qu'entre eux. Au contraire, nous souhaitons autant que possible proposer une réflexion qui soit intelligible par tous ;

- **Alerter** : l'actualité étant extrêmement mouvante sur ces sujets, nous publierons régulièrement des alertes sous forme de brève sur le site lorsque le droit positif évoluera sur ces sujets.

DOSSIER THÉMATIQUE

L'ÉDITORIAL DE JEAN-BAPTISTE SOUFRON

La stratégie juridique au cœur de l'innovation numérique

JEAN-BAPTISTE SOUFRON, ancien avocat, est le secrétaire général du Conseil national du numérique.

Il enseigne également à l'Ecole de Droit de Sciences Po.

On répète souvent en Europe que le droit serait en retard sur l'innovation.

Mais comment comprendre, alors, que les anglo-saxons soient si réticents face à ce qu'ils appellent « *preemptive legislation* », ou « réglementation anticipée » ? C'est parce qu'ils ont bien compris le rôle du droit dans l'environnement de la globalisation. Les modèles juridiques de leurs entreprises numériques sont étroitement imbriqués avec leurs modèles d'affaires et leurs modèles technologiques. Les arbitrages législatifs ne doivent pas être remis en cause car ils sont structurants et ont justifié d'importants investissements en temps et en argent.

Le juriste est piégé. Vouloir légiférer sur le droit des consommateurs en ligne, c'est anticiper et contrarier l'évolution technologique. S'abstenir de réglementer les algorithmes intrusifs, c'est donner l'impression que l'on est décalé avec l'actualité et se condamner à l'obsolescence.

La réponse à ce paradoxe oblige à redéfinir les termes du débat pour redonner une place centrale à la stratégie juridique, car c'est elle qui libère le développement des usages, les pérennise, garantit leur légitimité, et transforme l'innovation en progrès.

Ne dit-on pas aujourd'hui que les données sont le pétrole du numérique ? C'est reconnaître qu'un secteur économique tout entier s'est construit autour des données personnelles – objet juridique créé en 1978 dont le contrôle, la protection et le commerce dirigent de fait l'évolution technologique, contraignant, par exemple, les moteurs de recherche à inventer un outil permettant à tout usager européen de faire oublier les données qui le concernent.

Ne peste-t-on pas contre l'exploitation décrite comme abusive des directives sur le commerce électronique et la TVA par les géants du web ? Mais celles-ci sont essentielles à leur modèle d'affaire et leur permettent d'obtenir des avantages qui finissent par structurer le champ concurrentiel aussi sûrement que la plus brillante des innovations techniques.

Ne s'élève-t-on pas contre la méconnaissance par les usagers des conditions générales

d'utilisation et des licences des plateformes qu'ils utilisent au quotidien ? C'est parce qu'elles ont de plus en plus de conséquences dans leur vie personnelle – en rendant par exemple impossible la diffusion d'images comme le fameux tableau « *L'origine du monde* » qui a encore l'honneur des manuels d'histoire-géographie, mais dont la diffusion est largement censurée sur les réseaux sociaux.

Peut-on ainsi faire l'hypothèse que c'est le droit bien plus que la technologie qui formerait le cœur, l'âme et la sève de l'innovation numérique ?

Voilà peut-être le sens profond de la fameuse maxime de Lawrence Lessig, « *Code is Law* ». Ce n'est pas le droit qui est à la traîne du numérique. C'est le numérique qui revendique pleinement son statut d'autorité épistémique. La stratégie juridique y est tellement centrale que le président Obama lui-même s'est senti tenu récemment de mettre en garde les acteurs institutionnels européens face à la tentation d'une régulation trop rapide des grandes plateformes qui sont devenues l'un des fers de lance de son économie. Qu'il s'agisse de droit des robots, de consommation collaborative, d'usage des technologies par les salariés dans l'entreprise, du cloud, etc., les questions qui agitent ce secteur sont nombreuses et bouillonnantes d'originalité et d'énergie. Ce numéro de la Revue a l'ambition d'en donner une vision d'ensemble la plus large et la plus diverse possible.

Mais reste la question de comprendre la place du droit dans l'innovation. Et sur ce point, contrairement à ce que voudrait la théorie, les acteurs du numérique ne se demandent pas ce que devrait être le droit, mais comment il se crée et s'exerce, s'éloignant de toute forme d'intellectuallisme juridique, et assumant pleinement leur discours politique et idéologique. Peter Thiel, par exemple, le fondateur de Paypal et le premier investisseur de Facebook, ne manque pas de rappeler ses racines ultra-libérales et ne voit pas de contradiction à défendre simultanément le milieu des start-up en guerre contre les géants de l'industrie, et le principe du monopole comme moteur de l'innovation.

Cette vision ne fait pas d'opposition entre l'approche pratique et conceptuelle du droit. Personne n'a peur de construire, et chacun a bien le sentiment d'être dans un combat de concepts et d'idées. La notion de neutralité du net apparaît à l'improviste au moment où il est jugé nécessaire de permettre à Flickr et à Youtube d'utiliser sans surcoût les réseaux de télécoms à égalité avec les services des opérateurs. Et elle finit par s'incarner dans le réel à l'occasion de différentes lois en Europe et au Brésil, puis par une décision historique de la Federal Communication Commission. Quant à son concepteur, Tim Wu, il passe avec aisance d'une carrière universitaire de prestige à une candidature politique pour le ticket démocrate de l'État de New York – tout en s'offrant régulièrement l'avantage de disposer des pages du « New Yorker ».

Les exemples ne manquent pas. Porté par le succès des logiciels libres et des contenus collaboratifs, Lawrence Lessig a fait ressurgir des outils ancestraux comme le droit des communs pour rationnaliser leur régime et les fonder en droit au-delà du seul périmètre contractuel qui était initialement le leur. Motivé par les apports du Big Data, Cass Sunstein invente des passerelles entre le droit, la théorie de l'information et la psychologie behaviouriste en imaginant le concept du « *nudge* » et de la régulation algorithmique, c'est-à-dire en faisant l'hypothèse que le droit peut faire l'objet d'un design pour orienter directement les pratiques des citoyens. Il ne s'agit de rien d'autre que d'adapter le Code de la route pour

automatiser la sanction des radars routiers afin d'inciter les conducteurs à lever le pied. Mais cet effort visant à rattacher toute innovation concrète à un principe nouveau n'a rien d'anodin et correspond à une méthode qui se répète avec régularité.

Comprendre l'innovation est devenu le graal de nombreux entrepreneurs. L'enjeu est même devenu une question de survie depuis que des entreprises de tous secteurs confondus ont peur de se faire « uberiser ». Les brevets sont devenus des armes dans la guerre sans fin entre start-up, grands groupes et « *patent trolls* ». Le logiciel libre et les standards ouverts remettent en question les modèles de standardisation hérités des télécoms et de l'énergie. L'industrie des contenus a du s'adapter au développement du régime protecteur des plateformes. Des secteurs industriels entiers voient leurs économies menacées par l'apparition de nouveaux noms de domaine comme le .vin ou le .health. La banque et les marchés boursiers sont remués par le dynamisme du crowdfunding et des prêts participatifs.

Pour tous ces secteurs, la stratégie, c'est la capacité à créer sa différence, à se donner une valeur unique, grâce à laquelle le retour sur investissement sera plus important. Il ne s'agit pas tant de contourner les règles existantes, mais d'exercer son activité de façon originale.

L'exemple classique est celui d'Ikea, une société qui vise les clients jeunes qui veulent des meubles modernes sans dépenser beaucoup d'argent. En soi, c'est un objectif qui n'est pas différenciant pour Ikea car d'autres entreprises ont le même. Mais en décidant d'en faire sa stratégie, Ikea a choisi de redéfinir chacune de ses activités de façon unique pour que chacune d'entre elles respecte ce principe. C'est ainsi que Ikea s'est peu à peu doté de très nombreux services originaux à destination des jeunes couples, des cadres, des urbains, etc. Et c'est la collection de ces services construits autour de l'objectif de la société qui a fini par la différencier du simple magasin de meuble construit autour d'un parking. Ce ne sont pas ses meubles qui ont défini Ikea, c'est sa stratégie.

Les entreprises du numérique ne procèdent pas autrement, mais se différencient au moins autant sur le terrain juridique que sur celui du marketing. Wikipedia utilise avec originalité les règles du droit d'auteur pour permettre de construire une encyclopédie collaborative. AirBnB construit un système de logement partagé pour créer une nouvelle expérience d'hébergement, à mi-chemin entre chambre d'hôte et chambre d'hôtel. Uber interprète la réglementation des VTC pour proposer un service dont la qualité n'était pas à disposition des consommateurs auparavant.

Comme on peut le constater, la stratégie juridique est non seulement essentielle à chacun de ces projets, mais surtout, elle ne se contente pas d'appliquer le droit, mais elle le définit directement. Quoi de plus utile que de créer soi-même les catégories juridiques qui vous permettront de légitimer l'activité que vous questionnez ?

A ce titre, le droit n'est pas un acquis, et sa connaissance n'est pas une propriété qu'on peut exploiter à l'envi. En tant que pouvoir, le droit est une stratégie, et ses effets relèvent des techniques de dispositions, de manœuvres, de tactiques. Il s'exerce plutôt qu'il ne se possède. Il se pratique. Il n'est pas le privilège de ceux qui le connaissent et croient le posséder, mais le résultat d'un ensemble de positions stratégiques acquises dans le temps.

A la limite, confronté à l'innovation, le droit peut presque se comprendre comme une

collection d'illégalismes qu'il différencie en les formalisant. Il ne les oppose pas explicitement, mais offre aux uns le moyen de tourner les autres. Il les organise – les uns comme privilèges, les autres comme compensation. Le droit n'est plus un état de paix mais une guerre, dont l'évolution s'exprime par la stratégie de ses acteurs. La stratégie juridique de l'innovation exploite les foyers d'instabilité et crée des singularités pour leur permettre de se déployer. Elle repolitise nécessairement le droit et le contraint à s'extraire de la rhétorique technicienne.

C'est ce qu'ont bien compris les entreprises du numérique qui n'hésitent pas à faire appel à des juristes dans chacun de leur projet. De One Laptop A Child à la Khan Academy, les équipes de pilotage ne se contentent pas d'assembler des ingénieurs et des managers mais savent aller chercher le bon étudiant en droit ou le jeune *lawyer* qui sera au fait des pratiques et des astuces les plus récentes, celui qui aura le meilleur feeling pour trouver l'axe juridique autour duquel le projet pourra se construire, celui qui aura la meilleure stratégie.

Ce n'est pas un hasard si les penseurs critiques du numérique comme Jaron Lanier, Evgeny Morozov ou Lawrence Lessig ont tous un discours qui s'exprime en forme de stratégie juridique. Certains proposent de créer un régime de propriété personnelle des données pour résoudre l'inégalité des richesses dans l'environnement numérique. D'autres réfléchissent à des outils permettant de tracer chaque création originale afin de lui appliquer un micro-droit d'auteur, afin de rémunérer les nombreuses créations du public. On pourrait écarter ces propositions comme anecdotiques, péchant par excès d'originalité, ou par manque de rigueur juridique. Mais comment nier l'impact qu'ont aujourd'hui les Creative Commons sur des secteurs entiers comme l'édition ou la photographie ? Qui aurait pensé, il y a seulement un ou deux ans, que la loyauté des plateformes, l'autodétermination informationnelle, ou les données d'intérêt général, seraient au programme de la nouvelle Commission européenne ? Ce qui compte dans la stratégie juridique, ce n'est pas seulement le droit qui existe, c'est aussi le droit qui se crée.

Il ne s'agit pas pour autant de dire que le droit précède les usages, ni en principe, ni en pratique. En revanche, il faut comprendre que la stratégie juridique peut ouvrir une fenêtre de liberté pour ceux qui veulent imaginer des usages nouveaux, à condition de développer cette approche biface, pragmatique et conceptuelle à la fois, qui fait la force des anglo-saxons.

Personne ne le dit aussi clairement que Benjamin Edelman, qui reprend la maxime selon laquelle des excuses valent mieux que des regrets. Quand Youtube s'est lancé en 2005, ses cofondateurs se sont épargnés le processus de vérification des droits d'auteur sur les vidéos qui étaient mises en ligne. A l'inverse, les créateurs de Google Video s'efforçaient de vérifier tout ce qui était publié. Jawed Karim a justifié sa stratégie par une interprétation large des règles du droit d'auteur en ligne, finissant par mettre au point un outil de reporting pour déporter ce travail sur ces usagers plutôt que sur ses salariés. Tout cela s'est prolongé de façon complexe par un procès avec Viacom, un rachat de Youtube par Google et une série d'accord avec de nombreux ayants-droits. Mais après une période d'aller-retour, le droit s'est restructuré autour d'un nouveau paradigme correspondant à la stratégie choisie par la start-up californienne.

Cette attitude agressive a, bien sur, été favorisée par la sociologie du secteur. Le milieu universitaire a toujours été fortement représenté parmi les pionniers du numérique dont les niveaux socio-économique ou socio-culturel étaient très élevés. Se pose alors la question de

savoir si ces méthodes sont un enfermement ou une ouverture, une façon de recréer un entre-soi, ou un outil dynamique de prise du pouvoir par la confrontation des idées. Cet excès de stratégie ne risque-t-il pas de provoquer de trop fortes résistances et d'aboutir à des abcès juridiques et politiques ?

En réalité, l'importance de la stratégie juridique dans l'innovation est largement liée à l'importance de la technique dans la société. La tendance à la concentration et à l'automatisation accorde de plus en plus d'importance aux normes et aux processus, tout en laissant de plus en plus de marge à leur contenu lui-même. Face à de nouveaux procédés techniques dont la part va croissante dans la société, il est permis d'élaborer des règles nouvelles à condition de les penser de façon stratégique. Si ce phénomène n'apparaît pas au grand jour, c'est en grande partie parce ceux qui en sont les acteurs ou les spectateurs vivent dans la religion du fait et de l'instantanéité. Qui peut légitimement juger du caractère innovant du système de messagerie de Facebook par rapport à celui de MSN Messenger, ou à ceux qui l'avaient précédé ? On peut en revanche comprendre pourquoi le premier continue à se déployer tandis que le second relève du domaine de l'Histoire. La différence tient à ce que Facebook s'est doté depuis le départ d'une stratégie juridique relative aux contenus produits par ses usagers afin de pouvoir les utiliser au cœur de son modèle d'affaires – en les valorisant notamment à travers la publicité. Incarnée presque à regret dans les conditions générales d'utilisation du service, cette approche juridique ne choque pas les réglementations existantes, et n'en nécessite pas non plus de nouvelles. Elle est originale dans sa technique. Et elle est stratégique, car c'est autour d'elle que se définit l'ensemble des services de la plateforme.

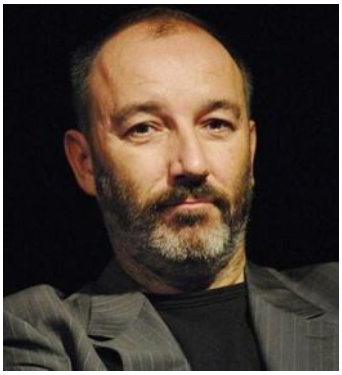
Cette volonté d'autonomie, fondée sur la stratégie juridique, se retrouve dès les origines du numérique. Elle figure en effet dès 1950 dans l'une des principales bibles de la Silicon Valley, écrite par Norbert Wiener et intitulée « *The Human Use of Human Beings* », c'est-à-dire « L'utilisation des êtres humains par d'autres humains » – et non pas « Cybernétique et société » comme le propose timidement la traduction française. Quelle plus belle démonstration d'un programme essentiellement stratégique, politique et juridique ?

Tout ce dispositif se traduit par une pratique très concrète de la stratégie juridique dans laquelle la rencontre des différents acteurs de l'innovation permet leur coadaptation. De nouveaux métiers comme les *chief innovation officers* apparaissent autour de ce besoin. Des think tanks ou des structures académiques hybrides, comme le Berkman Center, s'installent pour construire des idées. Des groupes de standardisation et de normalisation, comme le W3C, leur permettent de s'industrialiser. Des projets libres et ouverts garantissent la connexion à la société civile et à la recherche.

PIERRE BELLANGER

Principes et pratiques des données personnelles en réseau

Contribution à l'étude annuelle 2014 du Conseil d'État : « Le numérique et les droits fondamentaux »[1]



PIERRE BELLANGER est le fondateur et actuel président-directeur genéral de la radio Skyrock. Il est l'auteur de nombreux ouvrages et articles sur les développements technologiques liés au numérique dont le dernier s'intitule *La souveraineté numérique*[2].

RÉSUMÉ

« La reconnaissance de l'indivision en réseau des données personnelles et de leur statut de bien commun ; la reconnaissance des droits individuels et collectifs sur cette ressource ; la création d'une Agence des données pour les gérer ; la mise en pratique de ce dispositif légal par un triple chiffrement des données personnelles associé à des métadonnées de traitement ; un contrôle judiciaire et un contrôle contributif de la société civile sur les méthodes et procédures ; voilà qui apporte les garanties civiques nécessaires tout en accélérant le progrès et l'innovation par la mutualisation maîtrisée des données. »

Les données personnelles sont les informations renseignant, directement ou indirectement, sur un individu identifié. Cette définition établit un droit singulier de nature personnelle de l'individu concerné sur ses données, droit destiné à protéger, notamment, sa vie privée. Les réflexions juridiques et institutionnelles en cours tendent à vouloir renforcer et confirmer ce droit exclusif de chacun sur les données qui lui sont relatives. Les directions envisagées vont d'un droit autonome à en déterminer le recueil et l'usage, à une faculté indépendante d'administration – par la copie, la modification, le transfert ou la disparition partielle – jusqu'à, enfin, un droit de propriété privée par chacun de ses propres données personnelles.

Chacune de ces avancées a ses avantages et ses aléas. Mais correspondent-elles à la réalité des données personnelles d'aujourd'hui ?

[1] Conseil d'État, « *Étude annuelle 2014 du Conseil d'État - Le numérique et les droits fondamentaux* », La Documentation Française, septembre 2014.
[2] Pierre Bellanger, *La souveraineté numérique*, Éditions Stock, Paris, 2014.

En effet, ces dispositifs se fondent sur le présupposé que la donnée personnelle est autonome, ne renseigne que sur un seul individu, bref, considère la donnée personnelle comme granulaire, indépendante et formant une entité en soi, soumise au droit d'un seul.

Cette conception, pertinente jadis au temps des fichiers du XX^{ème} siècle, ne correspond plus à la réalité. Aujourd'hui, les données personnelles ne sont plus isolées, elles sont en réseau. Elles forment un réseau de données. Certes chacune demeure personnelle, mais elles sont désormais organisées en une totalité indissociable.

Et cela pour six raisons :

- **les données personnelles ne sont pas isolables en pratique** : donner accès à sa liste de contacts, à ses photos, à son agenda, à son courrier, à sa position, engage mécaniquement, de fait, les données personnelles d'autrui sur lesquelles on ne dispose d'aucun droit ;

- **les données personnelles renseignent sur d'autres personnes** : les algorithmes de corrélation, ces programmes informatiques qui permettent de déduire, par probabilité, des informations, par le traitement prédictif de masse de données sans rapport direct avec l'information inférée, font que chaque donnée personnelle renseigne indirectement sur autrui. Par exemple : les données personnelles de clients bancaires, croisées avec leur défaut de paiement, vont servir à déterminer le risque d'impayé de nouveaux clients, par la comparaison de leurs comportements. Par exemple encore : les données corrélées entre cancer du côlon et consommation en supermarché d'un groupe d'individus vont permettre de prédire le risque cancérogène d'une personne, sans relation avec le groupe témoin, et cela à partir de ses seuls tickets de caisse ;

- **les données personnelles sont une extension de la personne** : à la manière du sang, c'est un soi hors de soi. Engager le transfert ou la cession de données personnelles d'autrui, indissociables ou déductibles des siennes, en échange de l'accès « gratuit » à un service s'apparente par conséquent au trafic d'organes ;

- **le contrôle individuel par accord de gré à gré devient impossible** : les collecteurs de données personnelles sont destinés à se multiplier sous forme de capteurs disséminés partout, et intégrés dans la plupart des objets ; tandis, qu'à son tour, chaque individu devient collecteur de données sur lui-même et sur autrui. L'autorisation individuelle réfléchie à chaque captation, déjà aléatoire, n'est plus possible dans les faits. Le monde qui vient est un monde où tout incorpore de l'intelligence informatique, captatrice et communicante, par laquelle tout se traite et transite, afin de transmettre un flux permanent de données. La brosse à dents, la cafetière, l'automobile, le réfrigérateur, la montre, les lunettes, les vêtements, les chaussures, captent et se connectent. L'objet muet deviendra l'exception, l'environnement aveugle disparaît ;

- **la constitution d'un monopole des données personnelles** : l'effet réseau s'applique aux données personnelles ; la valeur d'une donnée est proportionnelle au carré du nombre de données auxquelles elle est reliée. En effet, la valeur d'une donnée provient de son contexte, apporté par des données supplémentaires.

Par exemple : l'achat d'une poussette renseigne sur la future consommation d'un foyer. Cette donnée unique a de la valeur pour tout annonceur publicitaire de produits destinés à la petite enfance. Mais une seconde donnée pourrait apprendre que l'achat de la poussette est un cadeau pour les voisins.

La donnée se vérifie, prend du sens et donc devient connaissance par son agrégation intelligente à d'autres. En conséquence, il n'y a pas valeur absolue de la donnée unitaire.

En revanche, le plus gros détenteur de données peut surenchérir sans cesse pour en acquérir de nouvelles, en numéraire ou en services gratuits, puisque c'est pour lui que les données ont le plus de valeur et que, de surcroît, chaque acquisition nouvelle accroît la valeur de l'ensemble déjà collecté, jusqu'à ce que, par cette logique, il en détienne le monopole ;

- **l'encadrement juridique de la modélisation informatique du réel** : la collecte globale et considérable de données – dont les données personnelles – constitue au final un tramage quantitatif de la réalité elle-même. L'appropriation par quelques entreprises de la reconstitution informationnelle du réel est source d'asymétries de concurrence dévastatrices et ne peut être empêchée par une somme de droits individuels.

  Par exemple : la connaissance directe ou prédictive par un seul acteur du type de conduite de chaque automobiliste lui donne un avantage décisif, et sans concurrence, pour établir des tarifs d'assurance auto sur mesure et au meilleur prix, sélectionnant ses clients pour ne laisser à sa compétition que les conducteurs qu'il a détecté comme non rentables. Ainsi, une somme d'acceptations personnelles sans conséquence immédiate pour les individus concernés pourrait mettre un terme au secteur de l'assurance tel que nous le connaissons, fonder de ce fait un nouveau monopole qui ne tarderait pas à renchérir l'assurance pour tout le monde.

Ainsi, les données personnelles ne sont plus granulaires mais réticulaires, c'est-à-dire organisées en réseau. Les données personnelles ne sont plus séparées mais liées. Cette intrication forme le réseau des données personnelles qui se substitue, en fait, aux données personnelles isolées du passé.

Comment se représenter le réseau des données personnelles ? L'hologramme est une bonne analogie : il provient d'une plaque photographique éclairée qui produit une image tridimensionnelle. Chaque morceau de la plaque contient l'image entière à moindre définition. De la même manière pour le réseau de données : la totalité des données reproduit le réel et chaque donnée renseigne sur l'ensemble.

Prenons un exemple : un seul grain de sable renseigne sur toute la plage, car la ressemblance entre la majorité des grains est forte. En revanche, un article provenant du rez-de-chaussée d'un grand magasin – un bracelet fantaisie – apporte peu d'information sur les articles de décoration ou de jardinage qui sont en étage. La plage est holonome : on peut déterminer l'information globale (la plage) à partir de l'information locale (le grain). Le grand magasin est autonome : chaque article ne détermine que lui-même.

Pour ce qui concerne l'être humain, il partage plus de 99 % de son génome avec les autres membres de son espèce, et son comportement, selon une étude de la revue Science, est à 93 % prévisible. Les données personnelles sont de fait holonomes.

Bien entendu, cette similitude et ces homogénéités de comportements n'ôtent rien au caractère unique de chaque humain – qui s'exprimera par d'infinies variations et par des marges surprenantes – ni à sa liberté, car son libre arbitre préserve à chaque instant son improbabilité. Il n'en demeure pas moins que cette singularité s'exprime en relation à une forte conformité à la moyenne, à une sorte de barycentre comportemental.

Ainsi la vision des données comme indépendantes et fondamentalement séparées les unes des autres est une abstraction qui n'est plus pertinente. Les données personnelles se déterminent mutuellement et forment un réseau organique.

De plus, ce réseau est dynamique. Le volume de données collectées double tous les 18 à 24 mois. Les données, jadis discrètes et donc isolables, deviennent des flux continus d'informations captées et quantifiées à chaque instant, liant en temps réel les données de sources individuelles multiples. Enfin, les liens logiques reliant les données entre elles se multiplient de manière exponentielle. Le réseau de données forme désormais une totalité animée en croissance permanente.

Par commodité, on appellera le réseau de données personnelles, le RDo.

Quelle est la nature juridique du RDo ? Il s'agit d'un objet sur lequel toutes les personnes, dont les données sont maillées, disposent de droits, mais qui ne peut être matériellement divisé entre eux. Il est ni dissociable, ni individualisable par nature, car chaque donnée personnelle renseigne sur les autres. C'est donc une forme d'indivision qui concerne toute la population.

Par ailleurs, les informations provenant du RDo sont d'un intérêt général majeur pour la collectivité, notamment, en matière de santé, de transports, de consommation, d'environnement ou encore de compétitivité économique.

Par son origine multi-personnelle, son impossibilité à le séparer, et son utilité collective, le RDo est donc un bien commun – *res communis* : un bien qui appartient à tous mais qui ne peut appartenir à personne en particulier. Son statut est défini en droit français par l'article 714 du Code civil[3].

C'est aussi un bien où chacun dispose de droits spécifiques (retrait, opposition, oubli) sur son propre apport et ce, dès lors qu'il n'engage pas les droits d'autrui.

Le RDo répond donc de droits collectifs et de droits individuels. La gestion et l'exercice de ces droits doit revenir à un organisme public, garant du contrôle démocratique et souverain, et seul à même d'en permettre l'accès et l'usage.

Une telle institution, structurante et référente, créé les procédures, les instances, ainsi que les

[3] « *Il est des choses qui n'appartiennent à personne et dont l'usage est commun à tous. Des lois de police règlent la manière d'en jouir.* »

concertations nécessaires. Elle devra donc, tout à la fois, gérer le bien commun et les droits individuels afférents. Sa capacité à ester en justice sera, de ce point de vue, essentielle.

Une agence des données pourrait ainsi être établie. La meilleure base ne serait-elle pas l'actuelle Commission nationale de l'informatique et des libertés (CNIL) ?

Quels droits individuels ?

La faculté technologique nouvelle de captation, de conservation et de traitement informatique des actes de chacun, tandis qu'en parallèle une part croissante de nos vies se déroule sur les réseaux et systèmes numériques, amène à définir – dans ce contexte – la nature et les droits en regard de la personne humaine.

Un être humain est à considérer comme un devenir permanent. C'est cette faculté et cette liberté de devenir qui le caractérise et doit donc être préservée voire accrue.

Le processus de ce devenir, parce qu'il est multiforme, contradictoire et sans limite, parce qu'il n'a de sens que dans un contexte profond et secret, se dénature s'il est observé par autrui, et donc jugé et normé. L'alchimie intime et solitaire n'appartient qu'à soi. Un des fondements de la personne humaine est donc le droit au mystère.

De ce processus personnel ressort un personnage que l'on s'est choisi ; cette représentation est une variante sociale de soi qui nous définit vis-à-vis des autres. L'intégrité de cette personne sociale doit être préservée. Ainsi, les informations individuelles accessibles, notre histoire personnelle, doivent par principe, et sauf exception motivée, répondre de la volonté individuelle de la personne concernée. C'est le droit au choix de soi.

La personne humaine, pour son accomplissement et la liberté de son évolution, doit se retrouver dans un environnement qui maximise ses choix. Toute réduction du champ des possibles, liée à sa nature réelle ou supposée, ne peut être qu'exceptionnelle, connue et motivée. Avec chaque réduction de choix éventuelle doit être proposée une alternative commune. C'est le droit à la neutralité du monde.

Par exemple : un site de commerce adapte, sans avertissement, son offre de produits en fonction de sa supposition du pouvoir d'achat de son client en ligne. Ce faisant, ce site limite la liberté de choix de son client potentiel pour orienter ses décisions et donc le conduire à un choix particulier qui ne serait pas forcément le sien, s'il avait accès à la totalité de l'offre. Cette restriction de choix est une atteinte à la liberté individuelle.

Les données personnelles sont une extension de la personne, et donc doivent être sous sa maîtrise. Sous réserve des prérogatives judiciaires, la souveraineté individuelle de chacun sur ses données personnelles est garantie.

Par exemple : une personne, dans le passé, a commis une infraction au Code de la route. Cette information disponible pour d'éventuels employeurs compromet bien des possibilités d'embauche. La personne doit avoir la faculté de réduire l'accès à cette information. Le passé ne doit pas être une prison, sauf dérogation temporaire et justifiée.

Enfin, l'accès aux données est un moyen formidable de développement de soi et des autres, équivalent à l'accès à la connaissance. Cet accès, s'il est conditionné par les droits précédents, doit être libre et ouvert à tous. C'est le droit d'accès aux données.

Par exemple : une personne souffre d'une affection peu répandue. Afin qu'elle exerce son jugement et détermine ses choix, l'accès aux données anonymisées de santé des autres malades pareillement atteints serait de la plus grande utilité.

Il faut noter que ces droits individuels sont d'utilité sociale. Qu'en serait-il de la création, de l'innovation, de l'entreprise, de l'imagination et donc du progrès collectif sans la garantie pour chacun de son intégrité informationnelle et la protection de sa liberté de pensée ?

Qu'en serait-il in fine de la démocratie sans ces droits qui sont à Internet ce que l'isoloir est à la République ?

Quels droits collectifs ?

Les données – dont font partie les données personnelles – lorsqu'elles sont utilisées par les programmes informatiques adaptés, constituent le meilleur moyen de réduire les gaspillages, les dysfonctionnements, les accidents, les pertes de la plupart des systèmes et organisations humaines. Les données sont au cœur de la résolution de nos difficultés actuelles, du progrès positif de nos sociétés, de l'épanouissement des individus, du redémarrage de notre économie, de l'emploi, de la santé et de l'environnement. En ce sens, à la manière du savoir scientifique, elles constituent un bien commun, non seulement par leur origine, lorsqu'il s'agit de données personnelles, mais par leur destination, ce qui en fait une cause d'utilité publique.

Par exemple : la moitié de la nourriture est gaspillée, notamment par le manque d'informations permettant le réajustement rapide des circuits de distribution. Un tiers de l'essence consommée est perdue en recherche de place pour se garer et donc par l'absence d'information à jour sur les emplacements disponibles. Et plus gravement, selon IBM, l'emploi des données permettrait de réduire la mortalité des patients hospitalisés de 20 pour cent.

Les privatisations rivales de données qui sont en cours nuisent au progrès général au sens où elles altèrent définitivement la concurrence. D'une part, par l'effet réseau, le premier acteur ne fera que se renforcer au détriment des autres et, d'autre part, soumettra au seul intérêt privé une ressource d'intérêt général.

C'est pourquoi, les partisans de la non-réglementation des données « pour favoriser l'innovation et la compétitivité » accomplissent, sciemment ou non, un contre-sens. Leur logique aboutit à l'éteignoir du monopole.

De même, l'individualisation juridique des données conduit à atomiser un droit collectif potentiel en une somme de droits privés plus facilement solubles : clic d'acceptation par clic d'acceptation.

Il n'est d'ailleurs pas étonnant que les entreprises du réseau les plus dataphages défendent séparément ou conjointement ces deux thèses : elles leur ouvrent grand les portes de la

domination absolue. La première thèse est une extension brute du règne mercantile. La seconde, plus subtile, en phase avec notre tradition juridique, se donne habilement l'allure d'un progrès.

En réalité, la compétition doit se faire, non pas sur l'appropriation des données, mais sur leur usage.

À chaque entreprise de concevoir les meilleurs programmes informatiques – les algorithmes les plus efficaces – pour en tirer le sens et la valeur. La vraie compétition équitable et productive est là. Ainsi doit être actée l'obligation de mutualisation des données, sous l'égide et la gestion de l'Agence des données, afin d'en permettre l'accès réglementé mais ouvert à tous.

Par exemple : les données recueillies par les thermostats intelligents à domicile peuvent servir aux pouvoirs publics, à l'industrie du bâtiment, aux artisans de l'isolation, aux architectes, aux fournisseurs d'énergie, aux particuliers et à l'ensemble des prestataires informatiques qui concevront les logiciels d'exploitation de ces données pour leurs clients. Laisser ces données aux mains d'un seul acteur, ou de quelques-uns, dévitalise des filières entières.

La reconnaissance de la nature en réseau des données personnelles fait qu'un individu n'a plus la faculté de consentir seul à la cession ou à l'accès à ses données personnelles. Toute captation ou traitement de données personnelles doit passer par un agrément de l'Agence de données, préalable à tout accord individuel.

Par exemple : une personne veut rejoindre un réseau social et lui confier l'accès à ses données personnelles. Elle ne pourra le faire que si ce réseau social est préalablement agréé par l'Agence des données, ce qui garantira tout à la fois ses données et celles d'autrui qu'elle engage forcément.

Par comparaison, un citoyen achète, de sa seule intention, un produit alimentaire ou un jouet du commerce, cependant la mise sur le marché de ces derniers répond d'une autorisation administrative antérieure.

Nous avons pris d'ailleurs l'habitude de cette sécurité pour la plupart de nos achats et nous l'étendons naturellement aux services en réseau qui pourtant n'en bénéficient pas.

Le transfert de données personnelles vers un service non agréé sera constitutif d'une infraction y compris à l'égard des personnes dont les données personnelles seraient impliquées.

Par exemple : une personne concède l'accès à son carnet d'adresses à un service de cartographie non agréé. Ce faisant, il livre sans autorisation les coordonnées de tiers qui pourront se retourner contre lui.

C'est donc cette Agence qui agréera toute captation de données sur le territoire national. Son statut public fonde une relation symétrique avec les grandes entreprises du réseau, plus équilibrée que les contrats d'adhésion souscrits d'un clic de souris par des particuliers pressés.

C'est l'Agence également qui agréera les dispositifs et logiciels permettant aux particuliers de recueillir les données personnelles d'autrui. Elle procédera également aux médiations et arbitrages pratiques entre citoyens, tout à la fois capteurs et captés.

Quelles sont les conditions de l'agrément de l'Agence des données ?

- la donnée personnelle doit être captée, conservée, traitée et transférée selon les protocoles et modalités fixées par l'Agence des données ;

- la captation, conservation, traitement ou transfert de données personnelles d'un citoyen européen répond des seules juridictions européennes, ce qui implique, de fait ou de droit, la localisation communautaire des serveurs informatiques ;

- l'exportation des données personnelles de citoyens européens hors du territoire de la communauté est limitée et taxée ;

- la régularisation de la situation fiscale du capteur au regard de l'activité réelle générée par l'usage des données personnelles captées sur le territoire national ;

- l'acceptation de la mutualisation des données sous le contrôle de l'Agence des données.

Quelles modalités pratiques pour le traitement des données personnelles ?

L'information sur un individu est source de valeur pour la collectivité. L'information sur un individu identifié est un risque privatif de liberté pour ce dernier. Il faut donc dissocier la personne (son identité), de son profil (les informations recueillies).

Pour atteindre cet objectif, il faut cesser de capter, traiter et transférer les données personnelles sans les protéger. Car toute information numérisée doit être considérée comme publique dès lors qu'elle n'est pas chiffrée. Cette aliénation de fait est une violation des droits individuels susmentionnés.

Ce chiffrement cryptographique doit donc garantir les droits individuels et collectifs afférents aux données sans pour autant en compromettre le meilleur usage.

Le chiffrement proposé est à triple clé. Chacune des clés ne permet le dévoilement que d'une partie seulement des éléments de la donnée.

Ainsi, une donnée est divisée en trois parties :

- *l'identifiant* : ce qui définit l'individu de manière unique ; comme son nom, son visage, toute signature biologique (rétine, ADN, voix, empreinte digitale, etc.) ;

- *le profil utilisateur* : ensemble des données relatives à un utilisateur ; le profil est propre à chaque service ou réseau de services ;

- *l'information* : renseignements impliquant au moins une personne ou un profil.

Ce qui se présente de la manière suivante :

Exemple de données personnelles captées et conservées par un musée :

- niveau I : *XXX-XXX-ACTION : une visite est comptabilisée par le Musée.*
- niveau II : *XXX-PROFIL-ACTION : DR589 a revisité le Musée.*
- niveau III : *IDENTIFIANT-PROFIL-ACTION : Karima Dubois a revisité le Musée.*

Le premier niveau est accessible en données publiques.

Les conditions de recherche et de traitement des données personnelles non identifiées sont restreintes par des seuils de granularité et de combinatoire évitant une précision révélatrice d'identité. Il s'agit de garantir l'incertitude sur les personnes identifiées par des tailles d'échantillon en maintenant ainsi un niveau de flou.

Par exemple : « Combien de personnes ont-elles un chien dans tel quartier ? » maintient l'incertitude, tandis que : « Combien de personnes ont-elle un chien dans tel immeuble ? » peut être divulgateur.

Par ailleurs, le rapprochement non autorisé entre une action, un profil et une identité devient un délit.

Le second niveau donne accès à l'historique du profil créé par le collecteur. Les conditions de cet accès sont déterminées par l'Agence des données, de telle manière à préserver le secret de l'identité des profils.

Pour le musée, son travail de statistique et de relations client est fait pour l'essentiel au niveau I et II.

Le troisième niveau n'est accessible que sur une décision judiciaire donnant accès à la clé cryptographique correspondante. Le Ministre de Justice deviendra ainsi le Garde des sceaux et des clés.

Pour le musée, les informations de niveau III qu'il génère – comme par exemple les données de paiement recueillie – sont exclusivement réservées aux seuls usages internes éphémères agréés par l'Agence, et ne peuvent faire l'objet d'aucun traitement externe, ou être partie prenante d'une quelconque transaction avec des tiers.

Cette donnée personnelle encapsulée dans un chiffrage à triple niveau sera associée à des données additionnelles, ou métadonnées, de deux ordres :

- les premières sont d'accès libre et indiquent les conditions d'utilisation des données personnelles, ainsi que les droits et restrictions spécifiques qui les accompagnent, instructions dont le respect est obligatoire ;

- les secondes constituent un historique de la capsule de données depuis son origine : c'est-à-dire la succession de toutes les opérations dont elle a été l'objet. Cette mémoire

associée fonde, par exemple, l'authenticité de la monnaie virtuelle Bitcoin, en l'espèce, par l'historique des transactions rattachée à chaque unité de compte. Cette partie est cryptée et sous contrôle de la clé judiciaire.

En fait, l'encapsulation et les métadonnées font ainsi désormais de la donnée personnelle, jadis inerte, une donnée intelligente.

La capsule peut être elle-même un agent logiciel – un petit programme informatique – qui se peut se comporter et réagir de façon autonome en fonction de contraintes et de conventions spécifiques.

Un exemple nous est donné par le système logiciel Ethereum : chaque donnée porte avec elle-même de manière décentralisée les conditions de son usage.

Par exemple : une donnée personnelle encapsulée dans un agent logiciel contenant une position de circulation d'un véhicule est accessible en niveau II aux services de gestion de trafic qui en ont besoin. L'agent logiciel qui reconnaît l'origine autorisée de la demande, l'authentifie, la valide, donne accès à la donnée, puis inscrit en métadonnées, la consultation de l'information.

L'agent logiciel pourra d'ailleurs être partiellement programmé par l'utilisateur à l'origine des données pour déterminer une relation spécifique d'accès limité avec des services agréés – sous réserve des droits de tiers – et ce, à la manière de la licence Creative Commons.

Les progrès fulgurants de la capacité des processeurs, du stockage, de la bande passante et de l'efficacité des algorithmes font que le surpoids issu de la protection des données, ainsi que des opérations informatiques associées, seront vite compensés.

Enfin, les machines devront prohiber par elles-mêmes les usages non autorisés des capsules de données personnelles comme, par exemple, des duplications ou des tentatives d'accès. Et ce, à la manière des photocopieurs ou des imprimantes qui interdisent la copie dès qu'elles reconnaissent que l'image à reproduire est un billet de banque.

L'Agence des données supervise et coordonne cette gestion globale des données. Aucune donnée n'est conservée par l'Agence.

Le code n'est pas ouvert pour garantir l'unicité et la sécurité des versions, éviter les malveillances et les abus, et garantir l'immédiateté des mises-à-jour et la stabilité. En revanche, l'ensemble des procédés, logiciels et méthodes de l'Agence est soumis à l'examen contradictoire et publié d'une *Cour des codes*.

Certaines parties des codes source peuvent cependant être examinées sur demande et ainsi ouvertes, tant à l'inspection qu'à l'amélioration, par le public à la manière du logiciel libre. Tous les codes, méthodes et protocoles, sauf exception limitée et motivée, sont à disposition de la Justice.

La reconnaissance de l'indivision en réseau des données personnelles et de leur statut de bien commun ; la reconnaissance des droits individuels et collectifs sur cette ressource ; la création

d'une Agence des données pour les gérer ; la mise en pratique de ce dispositif légal par un triple chiffrement des données personnelles associé à des métadonnées de traitement ; un contrôle judiciaire et un contrôle contributif de la société civile sur les méthodes et procédures ; voilà qui apporte les garanties civiques nécessaires tout en accélérant le progrès et l'innovation par la mutualisation maîtrisée des données.

Ces principes et pratiques des données en réseau sont applicables d'abord en France mais ont pour objectif la dimension européenne puis mondiale.

EMMANUEL BAUD & PHILIPPE MARCHISET[1]

La loi Evin à l'épreuve d'Internet

EMMANUEL BAUD, avocat associé, Jones Day

PHILIPPE MARCHISET, avocat, Jones Day, (Master droit économique - propriété intellectuelle, promotion 2010)

RÉSUMÉ

Promulguée le 10 janvier 1991 et retouchée à diverses reprises, la loi n°91-32 dite « Evin » demeure source de clivages politiques et de contentieux judiciaires nourris concernant la publicité des boissons alcooliques qu'elle encadre fortement. Si son régime de quasi interdiction de la publicité en faveur des produits du tabac fait l'objet d'un consensus assez large, ses dispositions relatives aux boissons alcooliques ont engendré de multiples difficultés d'application. La loi Evin pose, en effet, un principe d'interdiction de la publicité et de la propagande, tant directe qu'indirecte, en faveur des boissons alcooliques. La publicité n'est licite que si elle relève d'une liste limitative de supports ou de contextes[2], se borne aux seules mentions autorisées[3] et contient un message à caractère sanitaire.

INTRODUCTION

Jusqu'à la loi du 21 juillet 2009, Internet ne figurait pas parmi la liste des supports ou modes de communication autorisés par l'article L. 3323-2 du Code de la santé publique (« **CSP** »). D'apparence libérale, la réforme opérée par cette loi maintient un strict encadrement de la publicité en ligne. Par ailleurs, les réseaux sociaux et la multiplication des appareils connectés alimentent une jurisprudence trouble et peu prévisible pour les annonceurs. L'Association

[1] Cet article ne reflète que l'opinion de ces auteurs et n'engage aucunement le cabinet Jones Day ou ses clients.
[2] Article L. 3323-2 du Code de la santé publique (« **CSP** ») incluant, par exemple, l'affichage ou les fêtes et foires traditionnelles.
[3] Article L. 3323-4 du CSP visant, notamment, le mode d'élaboration ou les caractéristiques olfactives et gustatives du produit.

Nationale de Prévention en Alcoologie et Addictologie (« **ANPAA** »), à l'initiative de l'ensemble des contentieux judiciaires en la matière, n'a, quant à elle, toujours pas réussi à obtenir la sanction judiciaire de campagnes diffusées sur le réseau social Facebook. De leur côté, le Gouvernement et le Parlement s'interrogent sur l'opportunité d'une restriction accrue de la publicité en ligne, et ce malgré les préconisations en ce sens du Plan Cancer[4].

Plus de cinq ans après l'adoption de cette réforme (**I**), il convient de tirer les enseignements d'une jurisprudence incertaine en ce qui concerne le support Internet (**II**).

I. LA RÉFORME DU 21 JUILLET 2009

A. La légalisation de la publicité sur Internet

La loi Evin entendait limiter la publicité en faveur des boissons alcooliques mais a, en réalité, instauré un régime d'interdiction, au terme duquel seul ce qui est expressément autorisé est licite. En effet, la publicité a été autorisée par le législateur « *à titre exceptionnel* »[5] et seulement dans la mesure où elle serait objective et « *strictement informative* ». Autant de qualificatifs difficilement conciliables avec la notion même de publicité, nécessairement créative et évocatrice[6], et sa destination nécessairement méliorative, à défaut d'être incitative. Le Conseil constitutionnel, dans sa décision du 8 janvier 1991, a pourtant considéré la loi Evin conforme à la Constitution, au motif que le législateur « *a entendu prévenir une consommation excessive d'alcool* », notamment chez les jeunes, et « *s'est borné à limiter la publicité en ce domaine, sans la prohiber de façon générale et absolue* »[7].

Internet, moyen de communication inconnu du grand public au début des années 1990, a fait l'objet, lors de son développement, d'une relative tolérance concernant la publicité en faveur des boissons alcooliques. D'un point de vue juridique, il était tentant de voir en Internet un dérivé du Minitel envers lequel les parlementaires ne s'étaient pas montrés hostiles[8]. Par ailleurs, le Commissariat général au plan, auteur d'un rapport sur l'application de la loi en 1999[9], et le Bureau de vérification de la publicité (« **BVP** ») avaient laissé entrevoir la possibilité d'une réforme à court terme de la loi ou, à défaut, d'une interprétation extensive de la notion « *d'envoi par les producteurs […] de messages* » prévue par le 4° de l'article L. 3323-2 du CSP. Dans une telle optique, Internet n'était guère un support mais un simple moyen, transparent et neutre, qui ne pouvait donner prise qu'à un envoi, d'une part, et à un affichage, d'autre part. Autant de modes de communication *a priori* licites, correspondant au demeurant à la définition donnée par le législateur de la « communication au public en ligne » dans la loi n°2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique (« **LCEN** »)[10].

---

[4] *Plan Cancer 2014-2019*, présenté par le Président de la République le 4 février 2014, page 91, visant particulièrement la publicité sur Internet et les réseaux sociaux.

[5] Rapport n°1482 de l'Assemblée nationale annexé au procès-verbal de la séance du 20 juin 1990, p. 75.

[6] V. en ce sens la motivation d'un arrêt remarqué rendu par la Cour d'appel de Versailles le 3 avril 2014 sur renvoi après cassation (CA Versailles, 3e ch., 3 avril 2014, RG n° 12/02102, *CIVB c. ANPAA*).

[7] Conseil constitutionnel, décision n°90-283 DC.

[8] Sénat, Journal officiel du 13 décembre 1990, p. 5060.

[9] Rapport d'évaluation du commissariat au plan, octobre 1999.

[10] Article 1, IV de la LCEN: « *On entend par communication au public en ligne toute transmission, sur demande individuelle, de données numériques n'ayant pas un caractère de correspondance privée, par un procédé de communication électronique permettant un échange réciproque d'informations entre l'émetteur et le récepteur* ».

D'un point de vue plus structurel, le contentieux en la matière se focalisait essentiellement sur le contenu des campagnes (et notamment des campagnes d'affichage), ou encore sur la problématique de la publicité transfrontalière en faveur des boissons alcooliques lors des rencontres sportives.

Ce n'est qu'à compter de la fin de l'année 2007, et à l'initiative, une fois de plus, de l'ANPAA, que les juridictions ont eu l'occasion de couper court au vide juridique concernant Internet et de remettre en cause l'interprétation libérale de la loi qui, à défaut de réforme, avait prospéré. Ainsi, le Président du Tribunal de grande instance de Paris a, par ordonnance de référé du 8 janvier 2008, constaté, aux termes d'une lecture stricte de l'article L. 3323-2 du CSP, que la publicité faite par la société Heineken par messages électroniques diffusés sur le site www.heineken.fr emprunte un support qui ne relève pas de l'autorisation limitative établie par l'article précité[11]. La société Heineken avait, pour sa part, soutenu que « *la demande tendant à faire juger l'illicéité des publicités sur support Internet excède les pouvoirs du juge des référés* ». En appel, les magistrats ont tranché dans le même sens, au motif qu'« *il est manifeste […] que le support de l'Internet ne figure pas dans la liste limitative précitée* »[12]. À cette occasion, la Cour n'a pas manqué de rappeler l'orientation restrictive souhaitée par le législateur en mettant en avant le fait que la loi Evin inverse « *le principe traditionnel des libertés publiques, en édictant son oppose selon lequel toutes les mentions qui ne sont pas expressément autorisées par elles sont interdites* »[13].

Ces décisions Heineken ont suscité l'émoi auprès d'une partie des parlementaires, conduisant au dépôt de propositions de loi[14], puis d'amendements, lors de la réforme de l'hôpital prévue en 2009, et notamment un amendement n°80 présenté à l'Assemblée Nationale. Le souhait des parlementaires était d'autoriser la publicité sur Internet dans un objectif de sécurisation et d'adaptation de la loi Evin, ce que certains ont également pu considérer comme une hypocrisie au sein d'un texte visant à renforcer la santé publique.

Ainsi, l'article 97 de la loi n°2009-879 du 21 juillet 2009 portant réforme de l'hôpital et relative aux patients, à la santé et aux territoires a modifié l'article L. 3323-2 du CSP en ajoutant, au 9°, les « *services de communications en ligne* » comme supports publicitaires autorisés.

B. Une légalisation assortie d'exceptions

La légalisation de la publicité sur Internet souffre néanmoins de trois exceptions notables. Tout d'abord, sont exclus les services qui « *par leur caractère, leur présentation ou leur objet, apparaissent comme principalement destinés à la jeunesse* » et ceux édités par des associations sportives. Ces deux exceptions sont logiques au regard de l'intention initiale du législateur de prévenir des méfaits de l'alcool auprès de la jeunesse et de proscrire l'association de l'alcool avec le sport. Quoique logiques, ces exceptions, et notamment celle interdisant le ciblage de la jeunesse, n'en sont pas moins complexes à mettre en œuvre. Enfin, la dernière exception

[11] TGI Paris, Ord. référé,, 8 janvier 2008, RG n° 08/50061.
[12] CA Paris, 14ème chambre, section A, 13 février 2008, appel d'une ordonnance de référé, *Heineken*, RG n° 08/00245.
[13] CA Paris, 13 février 2008, précité.
[14] Proposition de loi n°219 relative à la publicité en faveur du vin sur Internet, enregistrée à la Présidence du Sénat le 27 février 2008.

prévue par ce texte prévoyant que la propagande ou la publicité ne doit être « *ni intrusive ni interstitielle* » est plus énigmatique encore.

Le périmètre de ces exceptions a été précisé par le ministère de la Santé, de la Jeunesse et des Sports à l'occasion d'une réponse à une question parlementaire[15]. Ainsi, le Ministre a souhaité que « *les sites destinés à la jeunesse ou dédiés au sport et/ou à l'activité physique (eux aussi fortement fréquentés par les jeunes)* » soient exclus – là où le texte borne l'interdiction aux seuls sites « *édités par des associations, sociétés et fédérations sportives ou des ligues professionnelles au sens du code du sport* », sans considération de leur contenu. Par ailleurs, le Ministre précise que « *les techniques intrusives comme les pop-ups (des fenêtres publicitaires qui surgissent de manière spontanée sur le Web), ou interstitielles (annonces, souvent animées voire sonores, qui apparaissent en cours de consultation d'une page et occupent tout ou partie de l'écran) sont prohibées* ». Cette définition est, d'ailleurs, inspirée du rapport précité du Commissariat général au plan qui définissait une technique interstitielle comme l'affichage de « *brefs messages s'intercalant entre deux pages de présentation d'un site* ». Ce croisement des définitions révèle qu'en 1999 une publicité interstitielle s'intercalait entre deux pages, là où, dix ans plus tard, elle apparaît en cours de consultation d'une seule page, nouvelle preuve de la difficulté de circonscrire les comportements considérés comme répréhensibles sur Internet, un support en perpétuelle et rapide évolution.

En 2010, les sociétés éditrices du site Internet dédié au whisky Glenfiddich et au parcours initiatique qu'il mettait en place ont eu les premières les honneurs de la jurisprudence. Tant en première instance, qu'en appel puis en cassation, le site dédié a été considéré – en partie – illicite, les juges ayant estimé que certaines expressions y figurant n'étaient pas rattachables aux mentions exclusivement autorisées par l'article L. 3323-4 du CSP.

Bien que le caractère éventuellement intrusif ou interstitiel de certains des éléments du site n'était pas directement en cause dans ces affaires, le Président du Tribunal de grande instance de Paris a profité du débat instauré à ce sujet pour rappeler que le caractère interactif d'un site « *ne libère pas l'émetteur de l'interdiction de ne pas transgresser les limites autorisées par la loi* »[16]. Cette précision n'est pas anodine dans la mesure où, déjà en 2010, Internet permettait *via* les techniques du Web 2.0 d'impliquer de manière accrue l'internaute dans l'affichage et le choix des contenus, non seulement dans l'apparition d'une banderole publicitaire, mais au sein d'un site entièrement dédié à une boisson alcoolique.

Les décisions Glenfiddich se focalisaient davantage sur l'appréciation de la licéité du contenu que sur ses modalités d'affichage ou les publics ciblés, lesquels n'ont commencé à être appréhendés en jurisprudence qu'avec les décisions rendues sur la campagne promotionnelle « Un Ricard, des Rencontres »[17]. Cette jurisprudence a ensuite évolué au gré des progrès technologiques, la notion de service de communication en ligne recouvrant tant le classique navigateur que l'application mobile.

II. LES ENSEIGNEMENTS DE LA JURISPRUDENCE SUR LES SPÉCIFICITÉS D'INTERNET

[15] Question n°34552, Journal Officiel de l'Assemblée Nationale, 27 octobre 2009, p. 10263.
[16] TGI Paris, Ord. référé,, 16 février 2010, RG n° 10/51504.
[17] Cass. Civ. 1ère, 3 juillet 2013 et CA Paris, 23 mai 2012, RG n° 11/56221, *Un Ricard, des rencontres*.

A. Les précautions indispensables pour les annonceurs et éditeurs de services de communications en ligne

L'apparition d'un nouveau mode de communication ou « *support* » licite n'en a pas fait perdre aux autres dispositions de la loi Evin leur pertinence concernant Internet. Ainsi, le contenu relayé *via* un service de communications en ligne, fût-il une bannière discrète présente sur un site tiers, doit demeurer respectueux des limitations en matière de contenus et d'affichage du message à caractère sanitaire. En outre, il est nécessaire que le message publicitaire soit clairement identifié comme tel ainsi que le dispose l'article 20 de la LCEN[18].

La nature du service de communications en ligne et le mode d'affichage et de défilement des informations sont à prendre en compte afin d'apprécier la licéité des mentions ou des éléments de la publicité. Ce fut le cas dans les décisions Glenfiddich qui ont considéré comme répréhensible la ritualisation du parcours de l'internaute autour du whisky *via* le site. Le film animé de la campagne « Un Ricard, des Rencontres », présent sur le site Internet dédié de la société Ricard et représentant le louchissement de l'eau dans l'alcool, fut lui aussi considéré comme illicite par le juge des référés. Les juges ont confirmé en appel l'illicéité intrinsèque des visuels, également présents en affichage et ajouté que « *la contrariété du film aux dispositions légales est encore plus patente, dès lors que la combinaison des éléments illicites relevés pour les affiches magnifie ces éléments à travers une mise en scène accentuée par la mobilité de l'image et une musique séductrice, l'ensemble aboutissant à une création esthétique destinée à donner à la boisson Ricard un caractère festif, incitatif à la consommation d'alcool* »[19]. Ces décisions, elles-mêmes confirmées en cassation, ont mis en exergue la nécessaire prudence que doivent adopter les annonceurs désireux d'utiliser de nouveaux outils technologiques, compte tenu des interprétations restrictives de la loi Evin. La Cour de cassation n'a d'ailleurs pas manqué de relever qu'un « consommateur jeune », cible prohibée des annonceurs, était « *particulièrement sensible aux nouvelles technologies* »[20].

Internet demeurant un espace où le libre accès est le principe, il est impératif que les annonceurs restreignent également l'accès aux sites Internet – en sollicitant l'internaute à déclarer son âge – mais aussi qu'ils opèrent un ciblage par pays. La jurisprudence a en effet pu considérer que le simple accès à un contenu litigieux ne suffit pas pour caractériser une violation de la loi. Ainsi, l'existence d'un filtrage par pays d'origine, nonobstant le fait que tout internaute puisse évidemment mentir sur son âge et son pays d'origine, suffit à démontrer qu'un site ne vise pas la jeunesse dès lors que par son caractère, sa présentation ou son objet, il n'apparaît pas comme principalement destiné à la jeunesse

[18] « *Toute publicité, sous quelque forme que ce soit, accessible par un service de communication au public en ligne, doit pouvoir être clairement identifiée comme telle. Elle doit rendre clairement identifiable la personne physique ou morale pour le compte de laquelle elle est réalisée* ».
[19] CA Paris, 23 mai 2012, RG n° 11/56221.
[20] Cass. Civ. 1ère, 3 juillet 2013, n° 12-22633.

B. Les zones d'ombre : réseaux sociaux et applications mobiles

En sus des sites Internet conventionnels, la jurisprudence a eu à se pencher sur deux nouveaux moyens privilégiés par les annonceurs pour promouvoir leurs produits, à savoir les réseaux sociaux, d'une part, et les applications mobiles, d'autre part, avec bien souvent une faculté d'interconnexion entre les deux.

Une première juridiction s'est prononcée sur la licéité même de publicités sur Facebook, en considérant le 6 janvier 2012 que, « *la publicité étant autorisée sur un service de communication en ligne, elle ne peut pas être interdite sur les réseaux sociaux tels que Facebook, dès lors que la société Moët Hennessy Diageo limite officiellement sa cible aux personnes âgées de plus de 21 ans* »[21]. La juridiction a constaté l'existence du ciblage paramétré par l'annonceur pour refuser d'y voir une publicité illicite ciblant la jeunesse.

Facebook est à cet égard symptomatique de la complexité des contentieux initiés à la requête de l'ANPAA et exposant les annonceurs à une certaine insécurité. Jusqu'ici l'ANPAA agissait systématiquement par la voie du référé, afin notamment d'obtenir une interdiction rapide de la poursuite d'un agissement qu'elle considère comme répréhensible. En contrepartie, le juge saisi est le juge de l'évidence et dispose de pouvoirs d'appréciation et d'interprétation moins étendus que le juge du fond. A deux reprises, l'ANPAA en a fait les frais et n'a pas réussi à faire interdire le recours à Facebook par des annonceurs. Dans ces affaires, l'ANPAA soutenait notamment que le réseau social Facebook, en ce qu'il était essentiellement utilisé par un jeune public, ne pouvait être employé à la faveur de publicités pour des boissons alcooliques. Or, tant l'application Facebook Ricard Mix Codes, téléchargeable sur mobile et utilisable *via* le réseau social[22], que la page Facebook dédiée à la boisson Desperados ont été reconnues licites par les juridictions après examen d'études sur la fréquentation de Facebook, non contestées par l'ANPAA, et grâce à la mise en place d'un système de filtrage d'âge[23].

Facebook a également été source de contentieux eu égard au caractère viral et communautaire de son interface, qu'il s'agisse des comptes, des pages ou des applications que ce service propose. L'ANPAA y a en effet vu un mode de publicité intrusif. Les messages relayés par le truchement d'une application au réseau d'amis de la personne inscrite ont ainsi été considérés comme des publicités, là où il était tentant d'y voir des correspondances privées. La Cour de cassation a approuvé la cour d'appel qui avait caractérisé « *en quoi le fait que ce message soit relayé par l'intervention d'un internaute à l'intention de son « réseau d'amis » ne lui faisait pas perdre son caractère publicitaire* »[24]. Cette décision de principe, concernant les seules applications, semble devoir être nuancée par une décision du président du tribunal de grande instance de Paris concernant la page Facebook Desperados, qui a considéré, le 20 février 2014, « *que l'utilisateur de Facebook ne peut pas recevoir de messages qu'il n'a pas sollicités, qu'il garde le contrôle en cliquant sur l'onglet 'j'aime' sur les informations qu'il souhaite recevoir et sur les personnes – en cliquant sur l'onglet 'amis' – auxquelles il désire communiquer ces informations ; que par suite, la publicité dès lors qu'elle est suscitée par l'internaute ne peut être qualifiée d'intrusive* ». Une telle motivation n'est pas sans rappeler une motivation similaire adoptée concernant le « Quizz J&B » à savoir que « *le jeu ne constitue pas un mode de publicité*

[21] TGI Paris, Ord. référé,, 6 janvier 2012, 11/59895, *Quizz J&B*, RG n° 11/59895.
[22] CA Paris, 23 mai 2012, RG n° 11/56221.
[23] TGI Paris, Ord. référé,, 20 février 2014, *Desperados*, RG n° 13/59661.
[24] Cass. Civ. 1ère, 3 juillet 2013, n° 12-22633.

intrusif, puisque c'est l'utilisateur qui télécharge lui-même l'application, ni interstitiel, puisque le jeu n'apparaît pas de manière intempestive […] et qu'il ne constitue donc pas une publicité ciblée »[25]. Facebook, par sa complexité et son caractère évolutif, demeurera encore longtemps au cœur des contentieux.

Les applications mobiles également ne seront pas en reste, tant l'interconnexion et le ciblage accru qu'elles permettent susciteront la suspicion de l'ANPAA.

Plus problématique est, en revanche, la définition même du terme « service de communications en ligne ». Une telle notion, qui à l'époque de son adoption n'avait pas anticipé l'explosion du phénomène des applications mobiles, pourrait rendre illicite une application disposant d'un fonctionnement autonome ne requérant pas Internet. En effet, la décision d'appel dans l'affaire « *Un Ricard, des Rencontres* » laisse entendre qu'un tel mécanisme, s'il était qualifié de publicité, serait illicite[26].

Cela implique-t-il qu'une application hors ligne donnant des recettes de cocktails ou un guide des vins puisse constituer une publicité ou une propagande illicite, en toute hypothèse, pour de l'alcool ? Pour mémoire, la Cour de cassation a défini la publicité ou la propagande en faveur d'une boisson alcoolique comme « *tout acte en faveur d'un organisme, d'un service, d'une activité, d'un produit ou d'un article ayant pour effet, quelle qu'en soit la finalité, de rappeler une boisson alcoolique sans satisfaire aux exigences de l'article L. 3323-4 du même code* »[27]. On voit naturellement dans cet exemple les limites, si ce n'est l'absurdité, de cette définition conférée à la publicité, et dont les effets juridiques sont contestables à d'autres endroits[28]. Il convient donc de militer en faveur d'un champ d'application de la loi Evin qui se cantonnerait à la seule publicité, laquelle devrait se définir comme un acte de promotion d'une boisson alcoolique, prenant place dans la conduite de l'activité d'une personne ayant un intérêt à promouvoir cette boisson alcoolique, et susceptible d'être perçu comme telle par une personne ou un public raisonnablement attentif. Une telle définition permettrait à certaines applications indépendantes des opérateurs économiques dans le domaine des boissons alcooliques de ne pas être qualifiées de publicité ou de propagande. Quant aux applications éditées par ces opérateurs, il conviendrait de les considérer comme licites dès lors qu'elles ont été installées au moyen d'Internet et donc « en ligne », indépendamment de leur autonomie par la suite.

De telles considérations n'ont certainement pas échappé aux magistrats qui ont pu juger récemment, par exemple, qu'un jeu à boire n'était pas manifestement illicite dès lors que « *la création d'un tel jeu comme sa distribution ne sont pas interdites et que le jeu en lui même ne*

[25] TGI Paris, Ord. référé, 6 janvier 2012, précitée.
[26] CA Paris, 23 mai 2012, RG n° 11/56221 : « *il n'est pas démontré que, après téléchargement nécessitant une connexion internet, cette application puisse s'exécuter de manière autonome, sans cette connexion ; qu'il sera, donc, retenu que cette application est, pour le juge de l'évidence, un service de communication en ligne* ». Dans cette espèce, les juges n'avaient pas considéré probants les éléments produits par l'ANPAA permettant de démontrer un fonctionnement autonome de l'application Ricard Mix Codes. Rien n'indique qu'une telle preuve était impossible.
[27] Cass. Crim., 3 novembre 2004, n° 04-81.123.
[28] V. la jurisprudence *Diptyque* de la Cour de cassation (Cass. Com., 20 novembre 2012, n° 12-11.753). Cf. également E. BAUD, P. MARCHISET, « Droit et jurisprudence du vin. Les marques trinquent aussi », *Revue des œnologues*, vol. 41, 2014, n°150, pp. 61-62.

constitue pas une publicité, même indirecte, à une des boissons alcooliques »[29]. Une telle application de la loi Evin doit être encouragée au nom de la sécurité juridique. Il est également important que les acteurs du domaine des boissons alcooliques puissent capitaliser sur le numérique et sur Internet, afin de promouvoir de nouveaux modes de consommation responsables et innovants. Sans renier les impératifs de la protection de la santé publique, les textes devraient pouvoir trouver à s'appliquer dans une certaine souplesse.

[29] Ord. référé, TGI Paris, 21 février 2013, *Happy Hour*, RG n° 13/51115.

PIERRE LUBET & SANDRINE CULLAFROZ-JOVER

La souplesse du droit face à l'usage croissant du BYOD : étude sur la gouvernance des données au sein de l'entreprise connectée

PIERRE LUBET, avocat associé, Altana

SANDRINE CULLAFROZ-JOVER, avocate, Altana

INTRODUCTION

« *Une circulation aisée des informations mettra un service meilleur, des décisions plus sûres, une adaptation plus rapide aux incitations et exigences du marché, à ce titre, l'informatique est une condition de croissance de l'entreprise, et, là encore l'enjeu est considérable d'autant plus qu'il se place dans un climat de concurrence plus âpre.* »[1]
Emile ROCHE

Une théorie de l'évolution. Par essence, la mise en œuvre de nouvelles technologies de l'information et de la communication au sein de l'entreprise emporte avec elle bon nombre de bouleversements dans l'organisation et la gestion des relations de travail. Ces mutations internes influencent substantiellement les rapports qu'entretiennent les acteurs de l'entreprise entre eux, mais également vis-à-vis de leur environnement : mieux la technologie est acceptée dans la vie quotidienne, plus elle trouvera à s'intégrer facilement dans le cadre du travail.

Les problèmes juridiques soulevés lors des principales étapes de l'informatisation des entreprises reflètent cette évolution de la perception des ressources informatiques par la société :

- **1ère étape - l'introduction des technologies de l'information (IT)** : l'entreprise

[1] E. ROCHE, Préface, in: P. LHERMITTE, « *Le pari informatique* », Paris, Editions France-Empire, 1968.

organise conventionnellement l'introduction de l'IT, tandis que le salarié fait l'apprentissage de l'utilisation des ressources informatiques au sein de l'entreprise ;

- **2ème étape – la démocratisation de l'IT** : les questionnements juridiques s'orientent vers l'encadrement de l'utilisation, par les salariés, des ressources informatiques de l'entreprise à des fins personnelles ;

- **3ème étape – la consumérisation de l'IT** : les questionnements juridiques s'inversent, et l'entreprise s'interroge sur l'utilisation des ressources informatiques personnelles, par les salariés, à des fins professionnelles ;

- **4ème étape – l'optimisation de l'IT dans le cadre de l'exécution du travail** : l'entreprise développe et optimise des outils informatiques collaboratifs, pour créer des interactions et stimuler l'intelligence collective. L'organisation juridique de cette mutation englobe des problèmes contractuels internes et externes : la question de la propriété intellectuelle des travaux réalisés en commun ainsi que celle des rapports entretenus avec les fournisseurs de solutions informatiques utilisées ne doivent pas être négligées ;

- **5ème étape – la mise en données de la gestion des ressources humaines de l'entreprise** : par l'exploitation des technologies de Big Data[2] l'entreprise cherche à définir des indicateurs de performance et à quantifier l'organisation du travail pour améliorer la gestion des ressources humaines. Une réflexion approfondie est alors menée sur la réglementation et la responsabilité liées au traitement de données personnelles servant de base au processus.

De la gouvernance de l'IT à la gouvernance des données. Au cœur de cette évolution, le rôle de la gouvernance des systèmes d'information s'est accru pour sécuriser les ressources informatiques – matérielles et logicielles – organiser le traitement des données au sein de l'entreprise, et mettre en place une stratégie d'administration.

A cet égard, les questions de propriété et de sécurité des données liées à la consumérisation de l'IT en entreprise favorisent un rapprochement interne entre les acteurs pour définir des règles et bonnes pratiques en vue de contribuer à la productivité du capital humain, et à la valorisation de données de qualité, considérés désormais en tant qu'actifs immatériels.

Le traitement juridique du B.Y.O.D.[3] (*Bring Your Own Device*) en entreprise, analysé sous le prisme de la gouvernance, permet ainsi d'envisager, non seulement les réponses juridiques à l'utilisation d'équipements initialement non répertoriés au sein de l'entreprise, mais également de participer à une réflexion plus générale sur la sécurité des systèmes d'information de l'entreprise (ou cyber stratégie) en vue d'améliorer sa compétitivité.

Définitions. Dans le cadre de cette étude, la notion de données doit être entendue sous son acceptation la plus large, et comprend l'ensemble des données techniques, commerciales,

[2] Lucie Lemoine, « *La mise en données de l'organisation du travail comme nouvelle voie de rationalisation managériale* », La lettre innovation et prospective de la CNIL, n°07, juin 2014.
[3] Aussi dénommé A.V.E.C. : « *Apportez votre équipement de communication* », Commission générale de terminologie et de néologie, Vocabulaire de l'informatique et des télécommunications, JORF, 24 mars 2013.

financières, et stratégiques susceptibles de créer de la valeur et de constituer le patrimoine informationnel de l'entreprise.

Le phénomène de consumérisation de l'IT repose sur l'utilisation d'un matériel informatique mobile permettant le transport, le stockage, l'échange et la consultation de données de toute nature, personnelles et professionnelles.

Pour une qualification juridique exhaustive, on peut distinguer (i) les équipements nomades non communicants (clés USB, disque dur externe), susceptibles d'être branchés sur du matériel d'entreprise, des (ii) équipements nomades communicants, susceptibles de se connecter à un réseau d'entreprise (smartphone, tablette numérique, ordinateur portable).

La popularité du phénomène est telle que plusieurs modèles économiques se sont développés quasi simultanément :

- le B.Y.O.D. : se dit de l'utilisation, dans un cadre professionnel, d'un matériel personnel, propriété du salarié, tel qu'un téléphone multifonction ou un ordinateur, sur lequel transiteront des données de l'entreprise. Le Code du travail dispose que l'employeur doit fournir au salarié le matériel et l'équipement nécessaires à l'exécution de sa mission[4]. Le recours au modèle du B.Y.O.D. ne peut donc reposer, en France, que sur le volontariat ;

- le C.O.P.E. *(Corporated Owned, Personnaly Enabled)* : se dit de la mise à disposition, dans un cadre privé, d'un matériel professionnel, propriété de l'entreprise et sélectionné par elle ;

- le C.Y.O.D. *(Choose Your Own Device)* : se dit de l'utilisation, dans un cadre privé, d'un matériel professionnel choisi par l'utilisateur au sein d'un catalogue d'équipements nomades ayant reçu l'agrément de l'entreprise.

Rapidement, le B.Y.O.A. (*Bring Your Own Applications*) a fait son apparition dans l'entreprise. L'expression désigne l'utilisation, dans un cadre professionnel, d'applications logicielles, généralement disponibles en mode SaaS [5], permettant notamment le stockage, la synchronisation et le partage d'un nombre infini de données (ex: Dropbox, iCloud, SkyDrive). Plus discrète, moins tangible, l'utilisation de ces solutions applicatives est plus difficile à identifier au sein de l'entreprise.

Dans le cadre d'une gouvernance de l'IT, le B.Y.O.A représente cependant un risque sécuritaire très important, dès lors que les données de l'entreprise côtoient potentiellement les données de plusieurs autres sociétés – voire mêmes celles de concurrents – dans un espace de stockage dont elle ne maîtrise pas l'étanchéité. Ainsi, selon des études statistiques récentes, environ 43% des cadres déclarent utiliser des applications personnelles de ce type à des fins professionnelles[6].

[4] Article L. 1222-1 du Code du travail.
[5] SaaS : software as a service (exploitation de logiciels via des serveurs distants).
[6] Etude IFP-GOOD Technology, 2012.

L'entreprise du 21ème siècle est connectée : les risques qui en résultent ne sont donc pas que théoriques et peuvent être répertoriés selon leur nature et leurs impacts.

Panorama des risques et enjeux. En premier lieu, les risques techniques peuvent être divisés en quatre sous-catégories : (i) la violation de la confidentialité des données de l'entreprise (pillage informationnel, divulgation accidentelle ou illicite, etc.), (ii) la violation de l'intégrité des données de l'entreprise (altération, modification accidentelle ou illicite, etc.), (iii) la violation de la disponibilité des données de l'entreprise (perte, destruction accidentelle ou illicite, etc.), et (iv) les atteintes aux systèmes d'information de l'entreprise *per se* (infection virale, destruction physique, bombe logique, déni de service, etc.).

En deuxième lieu, les risques juridiques résultent directement des manquements à des obligations légales et réglementaires de conformité, susceptibles d'engager la responsabilité civile et pénale de l'entreprise[7]. L'entreprise encourt également un risque juridique social du fait de la gestion de l'encadrement de l'usage de l'IT et de la relation employeur-salarié.

En troisième et dernier lieu, les risques économiques doivent s'analyser comme la conséquence de la réalisation des risques techniques et juridiques, et comprennent : les pertes financières dues à une mauvaise gouvernance, la réparation des préjudices causés à des tiers, la détérioration de l'image de l'entreprise sur un marché économique considéré et vis-à-vis de sa cible commerciale, la perte de chiffre d'affaires, etc. Ainsi, la consumérisation de l'IT, facilitant la mobilité des salariés et la portabilité des données, présente une menace interne à l'entreprise, qui doit se prémunir des vulnérabilités d'origine humaine et technologique.

Dans ce contexte, quelles sont les règles juridiques applicables à la sécurité des données au sein de l'entreprise connectée ?

Afin d'accompagner durablement les mutations technologiques au sein de l'entreprise, il apparaît nécessaire de nourrir une réflexion globale sur l'encadrement juridique de la sécurité des données dans un écosystème de mobilité (**I**). La connaissance des principaux instruments juridiques nécessaires à la poursuite des atteintes portées par le salarié à la sécurité des données (**II**) permettra, le cas échéant, ultérieurement de défendre le patrimoine informationnel et les intérêts économiques de l'entreprise.

I. ENCADREMENT JURIDIQUE DE LA SÉCURITÉ DES DONNÉES DE L'ENTREPRISE CONNECTÉE

Une gouvernance raisonnée. L'utilisation de ressources informatiques extérieures – initialement non maîtrisées par l'entreprise – pour stocker des données professionnelles représente une source de risques, à la fois pour la sécurité des systèmes d'information, mais aussi dans le cadre de la gestion du capital humain de l'entreprise. Aussi, une gouvernance raisonnée impose à l'entreprise de respecter une conjonction de règles applicables à la portabilité des données professionnelles (**A**), préalablement à la mise en œuvre d'un contrôle patronal de l'utilisation desdites données par les salariés connectés (**B**).

A. Règles de sécurité applicables à la portabilité des données professionnelles

[7] Voir sur ce point les développements de la Section I de la présente étude.

La technique et le droit. En matière de sécurité informatique, la technique et le droit entretiennent une intime complémentarité, qui tend de plus en plus à s'accentuer par l'adoption de normes légales et sectorielles visant à encadrer le traitement de données stratégiques ou sensibles. Comme le soulignait Bernard Teyssié, « *l'innovation technologique ne pèse plus uniquement sur le travail. Elle exerce aussi une pression sur la norme juridique qui l'organise et l'encadre.*[8] »

Les référentiels et recommandations techniques, émanant d'organisations internationales professionnelles[9] ou de services étatiques spécialement dédiés à la cybersécurité[10], aident donc l'entreprise à proposer et mettre en place des solutions pour gérer et sécuriser ses systèmes d'information ainsi qu'à améliorer ses pratiques managériales (**1**) en vue de répondre au renforcement des obligations légales applicables à la portabilité des données professionnelles (**2**).

1. Panorama des solutions techniques adaptées à la portabilité des données professionnelles

L'hygiène informatique à l'épreuve de la portabilité. En janvier 2013, l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) a publié un « Guide d'hygiène informatique » définissant les règles et pratiques nécessaires à maintenir la bonne santé des systèmes d'information des entreprises. Parmi les 40 recommandations de ce guide, certaines trouvent une application directe en matière de portabilité des données professionnelles, que ce soit par l'intermédiaire d'équipements nomades communicants ou non communicants.

Ainsi, l'ANSSI préconise l'adoption des mesures suivantes[11] :

- interdire la connexion d'équipements personnels aux systèmes d'information (ex : désactiver les ports USB, interdire les transferts de messages professionnels) (Règle n°5) ;

[8] B. TEYSSIÉ, « *Préface* », in M. DÉMOULAIN, Nouvelles Technologies et droit des relations de travail, Essai sur une évolution des relations de travail, Editions Panthéons-Assas, 2012.

[9] A titre purement informatif, les méthodologies considérées parmi les meilleures pratiques sont : la norme COBIT (*Control Objectives for Information and Related Technology*), la norme ITIL (*Information Technology Infrastructure Library*), les normes ISO 20000 et 27000 relatives à la sécurité informatique ainsi que la norme ISO/IEC 38500-2008 relative à la gouvernance des technologies de l'information.

[10] En France, l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) publie régulièrement de nombreux guides de bonnes pratiques. Le Centre d'Expertise Gouvernemental de Réponse et de Traitement des Attaques Informatiques (CERTA), qui dépend de l'ANSSI, publie quant à lui des avis et des alertes sur des vulnérabilités informatiques et tient à jour une série de recommandations visant à protéger les systèmes d'information.

[11] ANSSI, *Guide d'hygiène informatique*, 2013. D'autres règles sont également applicables en matière de gestion de la portabilité des données de l'entreprise, telles que : la règle n°1 (établir une cartographie des ressources technologiques), la règle n°15 (interdire techniquement la connexion des supports amovibles sauf si cela est strictement nécessaire et désactiver l'exécution des *autoruns* (exécution automatique de code) depuis de tels supports (Software Restrictions Policy)), la règle n°21 (mettre en place des réseaux cloisonnés), la règle n°23 (utiliser des applications et des protocoles de transmission sécurisés), la règle n°27 (définir les modalités d'analyse et de contrôle des événements journaliers).

- gérer les terminaux nomades selon une politique de sécurité au moins aussi stricte que celle des postes fixes (Règle n°17) ;

- chiffrer les données sensibles, en particulier sur les postes nomades et les supports amovibles (Règle n°19).

Par une approche sécuritaire maximale, la règle n°5 incite ainsi à bannir, purement et simplement, l'usage du B.Y.O.D., et à privilégier une flotte d'équipements nomades entièrement sélectionnés et maîtrisés par l'entreprise[12]. Ironiquement, la règle n°15 permet, malgré tout, d'envisager la connexion des supports amovibles (ex : USB) « *si cela est strictement nécessaire* ».

La popularité du B.Y.O.D. et du B.Y.O.A. impose toutefois à l'entreprise de tenter de concilier ces règles, qui relèvent d'une prudence drastique, avec une approche plus réaliste, pour sécuriser la portabilité des données professionnelles.

Des solutions technologiques. A la recherche d'un équilibre entre sécurité et portabilité des données, l'entreprise est préalablement contrainte de définir un modèle économique correspondant à des besoins réels. Quelque soit le modèle retenu (B.Y.O.D., C.Y.O.D, C.O.P.E), l'entreprise doit donc, à tout le moins, avoir connaissance des usages informatiques de son personnel afin de pouvoir en circonscrire les contours au sein d'une politique de sécurité adaptée et personnalisée.

Des outils logiciels de gestion permettent aujourd'hui de recenser et d'administrer la flotte des équipements nomades de l'entreprise, ainsi que les solutions applicatives utilisées par les salariés (*Mobile Device Management* et *Mobile Application Management*). A ce titre, il peut être recommandé à l'entreprise de fixer en amont des critères objectifs d'éligibilité des équipements – tel que la nature du système d'exploitation – ou de suggérer un paramétrage spécifique des fonctionnalités équipements.

L'entreprise a également la possibilité d'isoler les données professionnelles des contenus privés sur l'équipement du salarié, au sein d'un « silo », qui prend la forme d'une application ou d'un espace dédié, évitant ainsi le stockage anarchique de données professionnelles directement sur les équipements nomades personnels.

Ces méthodes doivent utilement s'articuler avec l'adoption de procédures de réversibilité des données de l'entreprise, notamment en cas de vol ou de perte d'équipement, ou encore dans l'hypothèse d'une rupture du contrat de travail du salarié. En tout état de cause, l'entreprise veillera à sécuriser tous transferts de données en privilégiant des passerelles ou des protocoles sécurisées, tels que VPN / HTTPS, afin d'éviter toute compromission des canaux de communications.

Une responsabilité structurelle. Au cœur de la gestion de la portabilité des données, se trouve, par conséquent, la question du contrôle des accès aux systèmes d'information de l'entreprise[13]. En pratique, celle-ci doit pouvoir justifier de la journalisation des connexions à

[12] Le C.O.P.E (*Corporated Owned, Personnaly Enabled*) est ici particulièrement visé.
[13] Voir également la délibération de la CNIL n° 81-094 du 21 juillet 1981, portant adoption d'une recommandation relative aux mesures générales de sécurité des systèmes informatiques.

son réseau et de la gestion des droits numériques des fichiers contenant les données professionnelles. La tenue rigoureuse des historiques participe à la traçabilité des opérations, dans le but de faciliter ultérieurement l'établissement et la conservation d'éléments de preuve des violations de sécurité.

Toutes ces précautions techniques engendrent une responsabilité structurelle qui repose essentiellement sur la direction des systèmes d'information de l'entreprise. Dès lors, l'entreprise doit prévoir en amont une définition claire des responsabilités de chaque intervenant qui participe à la mise en œuvre des mesures de sécurité. La rigueur de la rédaction des éventuelles délégations de pouvoirs au sein de l'entreprise pourront ainsi jouer un rôle essentiel pour définir les responsabilités de chacun dans un schéma plus large de délégation en cascade[14].

2. Renforcement des normes légales applicables à la portabilité des données professionnelles

Une origine sectorielle. La sécurité des systèmes d'information, qui tend à devenir une préoccupation plus juridique que technique, connait son origine et doit une grande part de son développement à des réglementations sectorielles. En matière bancaire et financière[15], par exemple, un corpus important de règles imposent aux entreprises des contrôles internes qui ont contribué à l'émergence d'une véritable gouvernance des systèmes d'information.

La sécurité des traitements de données à caractère personnel. Plus généralement, la loi informatique et libertés n° 78-17 du 6 janvier 1978 relative à l'Informatique, aux Fichiers et aux Libertés (modifiée) impose à tout responsable de traitement de données à caractère personnel de prendre « *toutes précautions utiles, au regard de la nature des données et des risques présentés par le traitement, pour préserver la sécurité des données et, notamment, empêcher qu'elles soient déformées, endommagées, ou que des tiers non autorisés y aient accès* »[16]. Cette obligation de sécurité et de confidentialité est, par ailleurs, pénalement sanctionnée à l'article 226-17 du Code pénal qui condamne par cinq ans d'emprisonnement et 300.000 Euros d'amende, soit 1.500.000 Euros pour une personne morale[17], « *le fait de procéder ou de faire procéder à un traitement de données à caractère personnel sans mettre en œuvre les mesures prescrites à l'article 34 de la loi n°78-17 du 6 janvier 1978 précitée* »[18].

[14] A toutes fins utiles, on rappellera que les délégations de pouvoirs permettent un mode de répartition et transfert de pouvoirs et de responsabilités civiles et pénales. Conformément à la jurisprudence de la Chambre criminelle de la Cour de cassation : « *sauf dans les cas où la loi en décide autrement, le chef d'entreprise, qui n'a pas personnellement pris part à la réalisation de l'infraction, peut s'exonérer de sa responsabilité pénale s'il rapporte la preuve qu'il a délégué ses pouvoirs à une personne pourvue de la compétence, de l'autorité et des moyens nécessaires* » (Cass. Crim., 11 mars 1993, n° 91-80.598 ; Cass. Crim., 11 mars 1993, n° 92-80.773 ; Cass. Crim., 11 mars 1993, n° 90-84.931 ; Cass. crim., 11 mars 1993, n° 91-83.655).

[15] Doivent être ici mentionnées : la Loi Sarbanes Oxley (SOX) du 30 juillet 2002 pour les entreprises cotées sur le marché américain ; la Loi n° 2003-706 du 1er août 2003 dite loi sur la Sécurité Financière en France ; le Règlement n° 97-02 du 21 février 1997 relatif au contrôle interne des établissements de crédit et des entreprises d'investissement (modifié).

[16] Article 34 de la loi « Informatique et Libertés » du 6 janvier 1978, modifiée par la loi du 6 août 2004.

[17] Article 131-38 du Code pénal.

[18] Article 226-17 du Code pénal.

Dans un contexte de portabilité des données, l'entreprise s'expose à voir sa responsabilité pénale engagée dès lors que le salarié peut accéder à des fichiers professionnels de données à caractère personnel (ex : fichiers de gestion des ressources humaines ou de clients et prospects) depuis un environnement informatique non sécurisé ne permettant pas de maîtriser les risques de perte, d'altération, de divulgation, ou de destruction – accidentelle ou illicite. Plusieurs hypothèses sont régulièrement constatées en pratique : accès au réseau de l'entreprise depuis un équipement nomade personnel vulnérable, transfert des fichiers de l'entreprise dans un espace de stockage en ligne ne présentant pas les modalités de protection adéquates (ex : messagerie en ligne, service de stockage et de partage de documents), etc.

La notification des failles de sécurité (*data security breach*) par les fournisseurs de services de communications électroniques. En cas de violation de la sécurité des données à caractère personnel, les opérateurs et fournisseurs de services de communications électroniques ouverts au public sont soumis à des procédures plus formelles et doivent impérativement :

- notifier sans délai :
    - la Commission nationale de l'informatique et des libertés (CNIL) de l'existence d'une violation ;
    - les personnes concernées, lorsqu'il y a un risque d'atteinte à la vie privée ou d'atteinte aux données à caractère personnel [19].
- conserver un registre des failles de sécurité et des mesures prises pour contenir leurs impacts[20].

Le législateur a assorti d'une condamnation pénale tout manquement au dispositif de notification susvisé, aux termes de l'article 226-17-1 du Code pénal[21].

De plus, il est intéressant de souligner l'ingérence possible du Ministre en charge du secteur des communications électroniques, qui peut désormais imposer des audits de sécurité chez les opérateurs[22].

Extension de l'obligation de notification à l'ensemble des entreprises. Favorable à une généralisation des obligations de sécurité des systèmes d'information, le projet de règlement européen portant réforme de la réglementation applicable à la protection des données personnelles envisage d'étendre l'obligation de notification des failles de sécurité à l'ensemble des secteurs d'activités[23].

---

[19] Article 34bis de la loi « Informatique et Libertés » du 6 janvier 1978 (modifiée), introduit par l'Ordonnance n° 2011-1012 du 24 août 2011 relative aux communications électroniques qui a pour objet, dans son titre premier, de transposer les directives 2009/136/CE et 2009/140/CE du Parlement européen et du Conseil du 25 novembre 2009.

[20] Idem.

[21] Article 226-17-1 Code pénal : « *Le fait pour un fournisseur de services de communications électroniques de ne pas procéder à la notification d'une violation de données à caractère personnel à la Commission nationale de l'informatique et des libertés ou à l'intéressé, en méconnaissance des dispositions du II de l'article 34 bis de la loi n° 78-17 du 6 janvier 1978, est puni de cinq ans d'emprisonnement et de 300 000 € d'amende* ».

[22] Article 6 de l'Ordonnance n° 2011-1012 du 24 août 2011 relative aux communications électroniques susvisée.

[23] Article 31 du projet de Règlement sur la protection des données personnelles.

B. Contrôle patronal de l'utilisation des données professionnelles par les salariés connectés

Responsabilisation de l'entreprise connectée. La souplesse offerte par le B.Y.O.D. implique une responsabilisation conjointe du salarié et de l'entreprise, qui doit assurer le contrôle de l'accès aux données et la surveillance de l'activité du salarié connecté (**1**). En particulier, l'entreprise devra prendre des mesures adéquates, y compris technologiques, pour contrôler le temps de travail et vérifier le respect des durées minimales de repos (**2**).

1. Contrôle de l'accès aux données et surveillance de l'activité du salarié connecté

La cybersurveillance à l'ère du B.Y.O.D. Aux termes de l'article L. 1121-1 du Code du travail, « *nul ne peut apporter aux droits des personnes et aux libertés individuelles et collectives de restrictions qui ne seraient pas justifiées par la nature de la tâche à accomplir ni proportionnées au but recherché* ». Cet article, qui réaffirme le droit à la protection de la vie privée au travail, impose à l'entreprise des limites dans le contrôle de l'accès aux données et la surveillance de l'activité du salarié connecté.

A l'ère du B.Y.O.D., la cybersurveillance est pourtant rendue d'autant plus nécessaire que l'accès aux données de l'entreprise est facilité à tout moment. Le pillage du patrimoine informationnel de l'entreprise est également favorisé par l'utilisation alternative ou conjointe de supports numériques de forte capacité, et d'espaces illimités de stockage et de partage de documents en ligne.

Dans ce contexte, il est essentiel de définir des bonnes pratiques au sein de l'entreprise ainsi que des modalités du contrôle permettant d'assurer effectivement la recevabilité des éléments de preuves d'un mésusage des ressources informatiques, personnelles ou professionnelles, par le salarié.

De la charte de bonne conduite à la charte informatique. L'autorité des instructions formulées par l'entreprise dépendra de la force contraignante qu'elle entendra leur donner (ex : note de service, charte de bonne conduite, ou charte informatique annexée au Règlement Intérieur), mais également de la réalité de leur contenu, qui peut :

- soit relever automatiquement du champ du Règlement Intérieur, dès lors que ce contenu présente une nature disciplinaire ;

- soit avoir la portée d'une simple déclaration morale peu contraignante.

Si le document est constitué, même pour partie, de dispositions relevant du champ du Règlement Intérieur, il ne peut être introduit qu'après avoir été soumis au Comité d'entreprise (CE) pour avis, et revu par l'inspection du travail qui peut demander des modifications ou le rejeter. D'une manière générale, il est recommandé de soumettre une telle charte au CE pour une bonne diffusion de son contenu auprès des salariés.

A l'exception des sociétés récemment formées, une charte informatique préexiste souvent à l'intégration de la problématique du B.Y.O.D. au sein de l'entreprise. Dans un tel cas, les mises

à jour nécessaires à l'encadrement des usages des équipements nomades sont également soumises à la procédure d'information et de consultation des organes de représentatifs du personnel.

L'information et la consultation des organes représentatifs du personnel. Ainsi, la mise en œuvre de nouvelles technologies et de mesures de contrôle de l'activité des salariés doit nécessairement faire l'objet d'une consultation du CE[24] – et le cas échéant du Comité d'hygiène, de sécurité et des conditions de travail (CHSCT)[25] – ainsi que d'une transmission à l'Inspection du travail[26].
Les dispositions d'un Règlement Intérieur portant sur l'utilisation des systèmes d'informations de l'entreprise ne seront pas opposables faute d'accomplissement des procédures préalables[27].

L'information préalable du salarié. De même, le salarié doit être informé des règles et des mesures de contrôle en vigueur au sein de l'entreprise, ainsi que des sanctions auxquelles il peut être exposé[28]. Les finalités du traitement relatif au contrôle de son activité doivent lui être clairement exposées. Il est fortement recommandé de conserver la matérialisation du consentement du salarié aux obligations de la charte informatique.

Les déclarations CNIL ayant pour finalité la gestion des systèmes d'informations et le contrôle de l'activité du salarié. La mise en œuvre de mesures de contrôle de l'activité du salarié, y compris de son accès aux systèmes d'information de l'entreprise, constituent un traitement de données à caractère personnel. Conformément à la loi « Informatique et Libertés », ce type de traitement doit faire l'objet de formalités préalables devant la CNIL. A défaut, l'entreprise n'est pas fondée à s'en prévaloir[29].

2. Contrôle du temps de travail du salarié connecté

La problématique du temps de travail du salarié connecté. L'utilisation des équipements nomades personnels communicants – de type smartphone ou ordiphone – permet au salarié de travailler à toute heure, en dehors de son lieu de travail. Dans un tel contexte, l'entreprise peut facilement perdre le contrôle et la maîtrise du temps de travail de son personnel.

Les risques liés au non respect des durées maximales de travail. La durée légale du travail effectif est légalement fixée à 35 heures par semaine civile pour l'ensemble des entreprises[30]. Ainsi, sauf dérogations[31], les durées de travail effectif ne doivent pas dépasser 10 heures par

[24] Articles L. 2323-13 et L. 2323-32 du Code du travail.
[25] Article L. 4612-9 du Code du travail.
[26] Article L. 2323-13 du Code du travail.
[27] Cass. Soc., 9 mai 2012, n °11-13.687.
[28] Article L.1222-4 du Code du travail.
[29] Cass. Soc., 6 avril 2004, n° 01-45.227 : « *à défaut de déclaration à la Commission nationale de l'informatique et des libertés d'un traitement automatisé d'informations nominatives concernant un salarié, son refus de déférer à une exigence de son employeur impliquant la mise en œuvre d'un tel traitement ne peut lui être reproché* ».
[30] Article L. 3121-10 du Code du travail.
[31] Les dérogations à la durée du travail sont accordées (i) par l'inspecteur du travail pour les demandes de dérogation relatives à la durée maximale journalière et (ii) par le directeur régional des entreprises, de la concurrence, de la consommation, du travail et de l'emploi (Direccte) ou, par délégation, le responsable de l'unité territoriale, ou par subdélégation, l'inspecteur du travail, pour les demandes de dérogation relatives à la

jour, 48 heures par semaine ou 44 heures en moyenne sur une période de 12 semaines consécutives. De plus, le salarié bénéficie d'un repos quotidien minimum de 11 heures par jour[32].

En cas de non-respect de ces durées maximales de travail, l'entreprise encourt une sanction pénale[33] et s'expose à un contentieux prudhommal. En effet, le salarié pourrait notamment formuler des demandes individuelles de rappels d'heures supplémentaires fondés sur des courriels envoyés ou des travaux réalisés en dehors du temps réservé au travail, voire même, prendre acte de la rupture de son contrat de travail au tort de l'employeur.

Les risques liés aux heures supplémentaires étendus à certains cadres au forfait-jour. Les risques liés aux heures supplémentaires concernent tous les salariés soumis aux 35 heures, équipés d'un équipement nomade communiquant, mais également certains cadres au forfait-jour. A ce titre, la Cour de cassation a récemment jugé que pour être valables, les forfaits-jours doivent faire l'objet d'un accord collectif contenant des dispositions de nature à garantir le respect des durées maximales de travail et les repos journaliers et hebdomadaires[34]. Cette interprétation jurisprudentielle stricte peut conduire à la reconnaissance de la nullité des forfaits-jours de l'entreprise et à sa condamnation au paiement de nombreuses heures supplémentaires[35].

Par conséquent, il est recommandé de consulter la convention collective et les accords d'entreprise applicables, afin de vérifier la présence de dispositions relatives aux forfaits-jours. A défaut de telles dispositions, la mise en place d'un accord collectif d'entreprise semble incontournable.

Les risques psycho-sociaux liés à l'hyperconnectivité du salarié. La consumérisation de l'IT est à l'origine de profonds bouleversements dans les conditions d'exécution du contrat de travail et fait peser une nouvelle responsabilité sur l'entreprise.

Notamment, l'usage du B.Y.O.D. et le déferlement des données professionnelles à toute heure confrontent le salarié à la réception massive d'informations et l'incite à être toujours plus disponible et plus réactif. Dans ces conditions, les temps de repos et de travail sont fongibles, constituant une source potentielle de déséquilibre[36], parfois qualifiée de « *stress électronique* »[37] en considération de la suractivité du salarié connecté.

---

durée maximale hebdomadaire. L'autorité administrative compétente est celle dont relève l'établissement qui emploie les salariés concernés par la dérogation (Instruction DGT n° 2010/06 du 29 juillet 2010).

[32] Article L. 3131-1 du Code du travail.

[33] Article R. 3135-1 et suivants du Code du travail : les pénalités relatives à la durée du travail sont de nature contraventionnelle (4ème et 5ème classe).

[34] Cass. Soc., 29 juin 2011, n° 09-71.107.

[35] Il convient de relever que certains secteurs d'activité se révèlent plus à risques que d'autres : Industries chimiques, Communications Electroniques. A contrario, des secteurs d'activité sont aujourd'hui couverts par un accord collectif valide en matière de forfaits-jours : Métallurgie, Syntec (depuis 2014).

[36] Le 2 juillet 2008, un accord interprofessionnel, étendu depuis 2009 (ANI du 2 juillet 2008 étendu par arrêté 23 avril 2009 (JO 6 mai 2009), définit le stress comme une situation de « *déséquilibre entre la perception qu'une personne a des contraintes que lui impose son environnement et la perception qu'elle a de ses propres ressources pour y faire face* » (art. 3, alinéa 1).

[37] Aurélia Dejean de La Bâtie, « *Gare au stress électronique !* », Les Cahiers Lamy du CE, 2009.

L'entreprise doit alors veiller à encadrer l'utilisation des équipements personnels, afin de prendre les mesures nécessaires pour assurer la sécurité et protéger la santé physique et mentale de son personnel[38]. Dans un avis du 14 mai 2013 sur les risques psychosociaux au travail, le Conseil Economique, Social et Environnemental a d'ailleurs expressément cité les TIC (Technologies de l'information et de la communication) comme « *cause interne à l'entreprise* ». A cet égard, la formation des responsables de services et chefs d'équipes aux problématiques liées à l'utilisation des équipements nomades et aux risques pesant sur l'entreprise est également cruciale.

Certaines entreprises ont déjà pris des mesures techniques pour limiter les connexions de leurs salariés à leur réseau en dehors des heures ouvrables. En interrompant ainsi la transmission des flux de données professionnelles sur les équipements nomades personnels de leurs salariés, ces entreprises ont instauré au sein de leur charte informatique un véritable « *droit à la déconnexion* »[39].

Plus récemment, un avenant de révision à l'accord national SYNTEC, étendu par arrêté le 26 juin 2014[40], a consacré une « *obligation de déconnexion des outils de communication à distance* ». Afin que le salarié respecte les durées minimales de repos, il est prévu que « *l'employeur veillera à mettre en place un outil de suivi pour assurer le respect des temps de repos quotidien et hebdomadaires du salarié* ». Il relève alors de la responsabilité de l'entreprise de s'assurer que le salarié peut techniquement se déconnecter des outils de communication mis à sa disposition et de surveiller que cette déconnexion est effective en pratique.

II. POURSUITE DES ATTEINTES À LA SÉCURITÉ DES DONNÉES DE L'ENTREPRISE CONNECTÉE

Une stratégie de défense protéiforme. Malgré la mise en place de mesures de protection adéquates, l'entreprise peut demeurer vulnérable aux atteintes internes (méprise, maladresse ou malveillance d'un salarié) et/ou externes (malveillance d'un tiers). Un arsenal juridique de protection varié permet alors à l'entreprise d'assurer la défense de ses intérêts en justice, dans un contexte de portabilité des données. Les mesures conservatoires et probatoires (A), précédant toutes actions à l'encontre du salarié fautif (B), permettent de réunir des moyens de preuve utiles. Parallèlement, des voies de recours répressives permettent à l'entreprise de poursuivre pénalement les atteintes à son patrimoine informationnel.

A. Mesures conservatoires et probatoires

Pour être en mesure de fonder ultérieurement ses prétentions et afin de garantir le respect de la protection de la vie privée du salarié (**1**), dans le cadre particulier de l'accès aux données professionnelles stockées sur des équipements nomades (**2**), l'entreprise peut faire établir des constats en matière informatique (**3**).

[38] Article L. 4121-14 Code du travail.
[39] Sophie Fantoni-Quinton, Céline Leborgne-Ingelaere, L'impact des TIC sur la santé au travail, La Semaine Juridique Social n° 48, 26 Novembre 2013, 1452 ; Jean-Emmanuel Ray, *Droit du Travail Droit Vivant*, Wolters Klumer, 23ème éd. 2014-2015, n°214.
[40] Avenant de révision de l'article 4 du Chapitre 2 de l'Accord National du 22 juin 1999 sur la durée du travail de la branche des bureaux d'études techniques, cabinets d'ingénieurs, conseils, sociétés de conseils (IDCC 1486), étendu par arrêté du 26 juin 2014 (JORF du 4 juillet 2014).

1. Le respect de la protection de la vie privée du salarié

L'admissibilité de la preuve en droit du travail. L'irrecevabilité de la preuve déloyale en droit du travail résulte de l'application de l'article 9 du Code de procédure civile, de l'article L. 1121-1 du Code du travail protégeant la liberté individuelle au travail, et de l'article 9 du Code civil, dernier rempart de protection de la vie privée de droit commun. Ainsi, les moyens de preuve obtenus à l'encontre d'un salarié fautif doivent répondre à un examen de proportionnalité et de finalité pour être admissibles devant des juridictions prudhommales, ce qui exclut la mise en œuvre de tout procédé clandestin. Cette exigence a donné lieu à une jurisprudence foisonnante sur le caractère privé des contenus stockés sur l'outil informatique mis à la disposition du salarié par l'entreprise.
Compte tenu de la supériorité des intérêts protégés[41], les moyens de preuves illicitement obtenus pourront, en revanche, être librement invoqués dans le cadre d'une procédure pénale.

Les développements jurisprudentiels sur le caractère privé des contenus du salarié. Traditionnellement, la jurisprudence s'est attachée à limiter le pouvoir inquisiteur de l'entreprise dans la recherche de moyens de preuves en définissant les contours du caractère privé de la correspondance électronique et des fichiers informatiques du salarié.

Dans le désormais célèbre arrêt Nikon, la Cour de cassation pose le principe selon lequel « *le salarié a droit, même au temps et au lieu de travail, au respect de l'intimité de sa vie privée ; celle-ci implique en particulier le secret des correspondances ; l'employeur ne peut dès lors prendre connaissance des messages émis par le salarié ou reçus 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 professionnel de l'ordinateur* »[42].

Depuis lors, la Cour de cassation a régulièrement pu affirmer le principe selon lequel les contenus des salariés, créés à partir de l'outil de travail mis à disposition par l'employeur, sont présumés professionnels, et peuvent être consultés par l'employeur, hors la présence du salarié et sans restrictions particulières[43]. Cette prérogative procède du pouvoir de direction de l'employeur qui est en droit de contrôler l'activité de ses salariés pendant leur temps de travail.

Il en résulte donc une obligation à la charge du salarié d'identifier expressément et d'intituler sans ambigüités comme « *personnel* » les contenus qui relèvent de sa vie privée. En revanche, un fichier informatique intitulé « *mes documents* » ne lui confère pas un caractère personnel[44]. La mention de son nom ou de ses initiales par le salarié ne suffit pas à renverser la présomption[45].

[41] Article 427 du Code de procédure pénale ; voir également la thèse de Matthieu Démoulain, « *Nouvelles technologies et droit des relations de travail – Essai sur une évolution des relations de travail* », Editions Panthéon-Assas, 2012, n°680 et suivants.
[42] Cass. Soc., 2 octobre 2001, n° 99-42.942.
[43] Cass. Soc., 18 octobre 2006, n°04-48.025 ; Cass. Soc., 19 juin 2013, n° 12-12.138 ; Cass. Soc., 26 juin 2012, n° 11-15.310; Cass. Soc., 8 décembre 2009, n° 08-44.840.
[44] Cass. Soc., 10 mai 2012, n° 11-13.884.
[45] Cass. Soc., 21 octobre 2009, n° 07-43.877.

L'accès aux contenus privés du salarié à partir de l'outil informatique de l'entreprise. La Cour de cassation maintient une jurisprudence constante et uniformisée, que ce soit en matière d'accès aux messages électroniques personnels ou en matière d'accès aux fichiers informatiques personnels : l'entreprise ne peut accéder aux contenus privés du salarié qu'en présence de celui-ci ou après l'avoir dûment appelé, sauf lorsqu'un risque ou un évènement particulier le justifie[46].

2. L'accès aux données professionnelles stockées sur des équipements nomades

Portée de la problématique. La question de l'accès aux données professionnelles stockées sur des équipements nomades se pose essentiellement pour le matériel dont le salarié est propriétaire (B.Y.O.D.). En effet, « *l'employeur ne peut porter atteinte à la propriété d'autrui, que ce soit en termes de contrôle du contenu, mais aussi lors du départ du salarié* »[47]. Toutefois, dans l'hypothèse d'une mise à disposition d'équipements nomades par l'entreprise (par exemple, dans le cas du C.O.P.E.), la difficulté d'assurer la protection des données professionnelles conserve tout son sens dès lors que le matériel considéré est en possession du salarié qui en détient la maîtrise effective jusqu'à sa restitution.

Dès lors, comment l'entreprise peut-elle accéder aux données professionnelles stockées sur de tels équipements ? **La position de la jurisprudence** est exprimé dans deux arrêts récents, rendus à l'occasion de contentieux impliquant l'usage par un salarié de son matériel personnel sur le lieu de travail, permettent d'envisager des éléments de réponse.

Dans un premier arrêt du 23 mai 2012[48], qui concernait l'accès par l'employeur au dictaphone personnel d'un salarié, la Cour de cassation a précisé que « *l'employeur ne pouvait procéder à l'écoute des enregistrements réalisés par la salariée sur son dictaphone personnel en son absence ou sans qu'elle ait été dûment appelée* ». Ainsi, l'entreprise ne peut accéder aux éléments contenus dans un équipement personnel qu'en présence du salarié ou celui-ci dûment appelé. Il est intéressant de souligner l'absence de mention de la possibilité d'accéder à l'équipement en cas de « *risques ou événement particulier* ». Cette mention, habituellement reprise par la jurisprudence pour justifier d'un risque d'atteinte aux systèmes d'information de l'entreprise, n'aurait effectivement que de rares causes de légitimité alors que l'équipement considéré n'est ni connecté au réseau, ni partie intégrante des ressources informatiques de l'entreprise.

Dans un second arrêt du 12 février 2013[49], qui concernait une clé USB personnelle connectée à l'ordinateur professionnel du salarié, la Cour de cassation a estimé que « *la clé USB, dès lors qu'elle est connectée à un outil informatique mis à la disposition du salarié par l'employeur pour l'exécution du contrat de travail, étant présumée utilisée à des fins professionnelles, l'employeur peut avoir accès aux fichiers non identifiés comme personnels qu'elle contient hors la présence du salarié* ». Dans l'hypothèse où l'équipement considéré est connecté au réseau ou relié aux systèmes d'information de l'entreprise, l'entreprise peut donc, même hors la présence du salarié, accéder aux contenus stockés non expressément identifiés comme « *personnel* ». Par

[46] Pour les fichiers informatiques personnelles : Cass. Soc., 17 mai 2005, n° 03-40017 ; pour les messages électroniques personnels : Cass. Soc., 10 juin 2008, n° 06-19.229 ; Cass. Soc., 23 mai 2007, n° 06-43.209.
[47] Jean-Emmanuel Ray, « *A propos de la révolution numérique* » (seconde partie), Revue de droit social, n°11-12, nov.-déc. 2012, p.1029.
[48] Cass. Soc., 23 mai 2012, n° 10-23.521.
[49] Cass. Soc., 12 février 2013, n° 11-28.649.

un mécanisme d'association, le rattachement de l'équipement aux ressources informatiques de l'entreprise lui confère ainsi une finalité professionnelle.

Par extrapolation, il ne pourrait être exclu que la jurisprudence reconnaisse à terme, pour l'administrateur réseaux de l'entreprise, le pouvoir d'accéder aux contenus privés en cas de « *risques ou événement particulier* », dès lors qu'il peut justifier que le rattachement de l'équipement considéré aux ressources informatiques de l'entreprise fait courir un risque de sécurité aux systèmes d'information de l'entreprise.

3. Les constats en matière informatiques

Le constat d'huissier. De sa propre initiative, l'entreprise peut recourir à un huissier pour « *effectuer des constations purement matérielles, exclusives de tout avis sur les conséquences de fait ou de droit qui peuvent en résulter* »[50]. Ainsi, le procès-verbal permettra d'établir la matérialité de faits objectifs, à l'exclusion de toute appréciation.

Le procès verbal de constat constitue un élément de preuve valablement admissible devant les juridictions. Les mentions intrinsèques du constat propres aux actes d'huissiers de justice font foi jusqu'à inscription de faux, tandis que les autres mentions relatives aux pures constations font foi jusqu'à preuve du contraire depuis la loi dite « Béteille » [51] du 22 décembre 2010[52].

En matière informatique, le procès-verbal de constat doit également contenir un ensemble de pré-requis techniques permettant de vérifier le mode opératoire utilisé[53] par l'huissier. Toute impression des copies d'écran descriptives dudit mode opératoire doit être personnellement réalisée par l'huissier. Le cas échéant, le procès-verbal pourra se voir dénier toute force probante par les juridictions[54].

Le recours à l'article 145 du Code de procédure civile. L'entreprise a également la possibilité, pour contourner la protection accrue des contenus privés du salarié, de solliciter – par voie de requête ou de référé – une mesure d'instruction *in futurum* sur le fondement de l'article 145 du Code de procédure civile[55]. Le texte présente principalement l'avantage de permettre à l'entreprise de procéder par voie de requête, c'est-à-dire suivant une procédure non contradictoire, pour autant que les circonstances de l'espèce le justifie.

Dans un arrêt Datacep du 23 mai 2007, la Chambre sociale de la Cour de cassation a jugé que le respect dû à la vie personnelle du salarié ne faisait pas obstacle à l'application de l'article 145 du Code de procédure civile.

---

[50] Article 1er de l'ordonnance n°45-2592 du 2 novembre 1945 relative au statut des huissiers.
[51] Loi n° 2010-1609 du 22 décembre 2010 relative à l'exécution des décisions de justice, aux conditions d'exercice de certaines professions réglementées et aux experts judiciaires.
[52] Sur ce point, voir Joël Mazure, « *Constat d'huissier de justice : quelle force probante ?* », Revue de l'Habitat, Avril 2012.
[53] La norme AFNOR NF Z67-147 relative au « *mode opératoire de procès-verbal de constat sur Internet effectué par huissier de justice* » définit le mode opératoire que devrait suivre l'huissier afin de garantir que son constat soit le plus fiable possible. Cette norme n'a cependant pas un caractère obligatoire et ne saurait être invoquée seule pour contester la validité d'un procès-verbal (CA Paris, Pôle 5, Ch. 1, 27 février 2013).
[54] TGI Paris, 16 octobre 2009, Keepschool / KP média accessible sur LEGALIS à l'adresse url suivante : http://www.legalis.net/spip.php?page=jurisprudence-decision&id_article=2850.
[55] Cass. Soc., 23 mai 2007, n° 05-17.818 ; dans le même sens : Cass. Soc., 10 juin 2008, n° 06-19.229.

L'application de l'article 145 du Code de procédure civile[56] suppose néanmoins la réunion des 3 critères de recevabilité suivants :

- que le requérant initial détermine spécifiquement la **nature des mesures d'investigations** sollicitées ;

- que le requérant initial vise le **texte légal ou réglementaire** permettant de fonder les mesures sollicitées ;

- que le requérant initial précise le **caractère nécessaire et proportionnel** des mesures sollicitées.

Sous réserves de caractériser un motif légitime, une stratégie processuelle peut, de ce fait, être mise en place pour permettre à l'entreprise d'appréhender le contenu de l'équipement personnel d'un salarié (de type B.Y.O.D.), sans s'exposer au risque de destruction d'éléments de preuves compromettants par ce dernier.

Toutefois, le caractère non contradictoire de cette procédure n'exclut pas la présence du salarié au moment de l'exécution de l'ordonnance obtenue. Dans un telle hypothèse, la Cour de cassation a déjà jugé que « *l'employeur avait des raisons légitimes et sérieuses de craindre que l'ordinateur mis à la disposition de la salariée avait été utilisé pour favoriser des actes de concurrence déloyale, a pu confier à un huissier de justice la mission de prendre copie, en présence de la salariée ou celle-ci dûment appelée et aux conditions définies par le jugement confirmé, des messages échangés avec des personnes identifiées comme étant susceptibles d'être concernées par les faits de concurrence soupçonnés* »[57].

B. Actions à l'encontre du salarié fautif

Types d'actions envisagées. L'atteinte portée à la sécurité et à la confidentialité des données de l'entreprise peut naturellement trouver son origine dans la maladresse ou la malveillance d'un salarié, mais également par la malveillance d'un tiers, qui aura malicieusement exploité les failles de sécurité des systèmes d'information de l'entreprise, y compris les vulnérabilités liées à l'intégration des B.Y.O.D. Cependant, dans le cadre de cette étude des rapports internes à l'entreprise sur l'usage des B.Y.O.D, seules les actions à l'encontre du salarié fautif feront l'objet d'une analyse. Ainsi, en cas de malveillance dans l'accès aux données de l'entreprise, l'entreprise pourra sanctionner le salarié (**1**), et/ou exercer une action devant les juridictions pénales (**2**).

1. Sanction à l'encontre du salarié fautif

Le licenciement pour faute grave. Le salarié fautif qui aura volontairement ou par une négligence impardonnable porté atteinte aux données de l'entreprise pourra être licencié pour faute grave. Le licenciement pour faute nécessite l'application de la procédure disciplinaire.

[56] Article 145 du Code de procédure civile : « *S'il existe un motif légitime de conserver ou d'établir avant tout procès la preuve de faits dont pourrait dépendre la solution d'un litige, les mesures d'instruction légalement admissibles peuvent être ordonnées à la demande de tout intéressé, sur requête ou en référé* ».
[57] Cass. Soc., 10 juin 2008, n° 06-19.229.

Selon la jurisprudence, la « *faute grave* » est caractérisée lorsque le salarié commet une faute d'une importance telle qu'elle peut seule justifier une mise à pied conservatoire, et rend impossible son maintien dans l'entreprise[58], y compris pendant la durée du préavis[59]. Par conséquent, le salarié ne bénéficie plus de son droit à l'indemnité de licenciement ni à l'indemnité de préavis[60] mais conserve son droit aux congés payés (par opposition au salarié licencié pour faute lourde).

L'entreprise est obligée de suivre une procédure stricte pour que le licenciement opéré soit régulier. A ce titre, la mesure de mise à pied conservatoire[61] est, en principe, prononcée dans le cadre d'une procédure de licenciement pour faute grave[62] : le salarié de l'entreprise concernée ne peut plus se rendre sur son lieu de travail, le contrat de travail étant suspendu dans le but de préserver la sécurité des systèmes d'information de l'entreprise.

Applications jurisprudentielles. Les juridictions ont d'ores et déjà estimé que constituait une faute grave toute entrave aux limitations et gestion des droits d'accès établies par l'entreprise. Par exemple, le fait d'emprunter un mot de passe pour se connecter au poste informatique d'un tiers[63] ou de divulguer des codes à des salariés non habilités ou à des tiers constitue une faute grave[64].

De même, en matière d'utilisation de périphériques, la Cour d'appel de Riom a jugé que le licenciement du salarié, à qui il était reproché d'avoir consulté des données de nature confidentielle et de les avoir transférés sur une clé USB, reposait sur une faute grave[65].

Par conséquent, peut être caractérisée de faute grave et faire l'objet d'un licenciement, toute atteinte au patrimoine informationnel de l'entreprise, résultant de l'utilisation d'un équipement personnel nomade, ou résultant de l'accès aux systèmes d'information de l'entreprise en violation de l'habilitation expressément donnée par l'administrateur des systèmes de l'entreprise.

2. Action répressive à l'encontre du salarié fautif

La pluralité des fondements. La divulgation intentionnelle d'éléments confidentiels du patrimoine informationnel de l'entreprise peut être sanctionnée sur la base de plusieurs fondements[66]. Il n'est pas question ici d'en dresser un catalogue exhaustif, mais de mettre

[58] « *La faute grave résulte d'un fait ou d'un ensemble de faits imputables au salarié qui constitue une violation des obligations résultant du contrat de travail ou des relations de travail d'une importance telle qu'elle rend impossible le maintien du salarié dans l'entreprise pendant la durée du préavis* » (Cass. Soc., 26 févr. 1991, n° 88-44.908).
[59] Cass. Soc., 27 septembre 2007, n° 06-43.867.
[60] Articles L. 1234-1 et L. 1234-9 du Code du travail.
[61] Article L. 1332-3 du Code du travail.
[62] Cass. Soc., 6 nov. 2001, n° 99-43.012.
[63] Cass. Soc., 21 décembre 2006, n° 05-41.165.
[64] Cass. Soc., 5 juillet 2011, n° 10-14.685.
[65] CA Riom, chambre civile 4, 12 Février 2013, n° 11-01.747.
[66] Par exemple : Violation du secret professionnel (article 226-13 du Code pénal) ; Violation du secret de fabrique (article 621-1 du Code de la propriété intellectuelle) ; Violation des secrets de fabrication (article L. 1227-1 du Code du travail) et bientôt Violation du secret des affaires (Projet de loi portant sur la protection du secret des affaires n°2139, Assemblée nationale, 16 juillet 2014).

l'accent sur des infractions particulièrement propices à la poursuite des atteintes à la sécurité des données de l'entreprise connectée.

Les notions de « *vol de données* » et d' « *abus de confiance* ». Le vol est caractérisé par « *la soustraction frauduleuse de la chose d'autrui* »[67]et est puni de trois ans d'emprisonnement et de 45 000 euros d'amende[68]. Le « *vol d'informations* » ou « *vol de données* » est ignoré du Code pénal et ne constitue pas en tant que telle une infraction. Au contraire, l'élément matériel de la qualification du vol renvoie expressément à la soustraction d'«*une chose* » corporelle et tangible.

Néanmoins, les juridictions ont déjà jugé que l'information pouvait faire l'objet d'un vol[69], pour autant que celle-ci soit reproduite sur un support, dont la soustraction serait l'objet du délit[70]. Ainsi, bien que traditionnellement perçue par les juristes comme le parent pauvre de la répression des infractions via les nouvelles technologies, la qualification de « vol » semble pouvoir retrouver une nouvelle source d'interprétation sur le terrain du B.Y.O.D. En effet, la copie de données confidentielles sur un équipement périphérique personnel devrait permettre de caractériser le support nécessaire à l'application du texte pénal.

La qualification d' « *abus de confiance* »[71] sanctionne quant à elle « *le fait par une personne de détourner, au préjudice d'autrui, des fonds, des valeurs ou un bien quelconque qui lui ont été remis et qu'elle a acceptés à charge de les rendre, de les représenter ou d'en faire un usage déterminé* ». L'abus de confiance est puni de trois ans d'emprisonnement et de 375.000 euros d'amende. La référence à la notion peu précise de « *bien quelconque* » permet, en effet, de couvrir a priori l'ensemble des données informatiques pouvant représenter une valeur économique pour l'entreprise. Ainsi, la Cour de cassation a jugé que « *les informations relatives à la clientèle constituent un bien susceptible d'être détourné par un salarié et caractériser un abus de confiance* »[72].

En tout état de cause, il faut considérer ces infractions comme complémentaires, dans le cadre du traitement juridique des B.Y.O.D. : dans un jugement du 26 septembre 2011, le Tribunal correctionnel de Clermont-Ferrand a condamné, pour vol et abus de confiance, une salariée ayant transféré des fichiers confidentiels sur une clé USB, le jour de son départ de l'entreprise, afin de les utiliser à des fins personnelles[73].

La notion d' « atteinte à un système de traitement automatisé de données ». Une liste d'infractions sanctionne les atteintes à un système de traitement automatisé de données (STAD) aux articles 323-1 et suivants du Code pénal, parmi lesquelles :

- l'intrusion frauduleuse et le maintien dans un STAD ;

[67] Article 311-1 du Code pénal.
[68] Article 311-3 du Code pénal.
[69] Cass. Crim., 4 mars 2008, n° 07-84.002.
[70] Relevons qu'ici la soustraction de l'information, duplicable par nature, n'emportera pas nécessairement dépossession de son propriétaire initial.
[71] Article 314-1 du Code pénal.
[72] Cass. Crim., 16 novembre 2011, n° 10-87.866.
[73] TGI Clermont-Ferrand, Ch. Corr., 26 septembre 2011, voir commentaire de É. A. CAPRIOLI, « *Condamnation pour vol et abus de confiance d'une ex-salariée ayant transféré des fichiers sur une clé USB* », Communication Commerce électronique n° 3, Mars 2012, comm. 36.

- l'entrave au fonctionnement d'un STAD ;

- l'introduction frauduleuse de données dans un STAD.

Les condamnations applicables ont été successivement renforcées par les lois n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique, et n° 2012-410 du 27 mars 2012, relative à la protection de l'identité. Les peines oscillent ainsi entre 2 à 7 ans d'emprisonnement et entre 30.000 euros et 100.000 euros d'amende.

Dans le cadre de la gestion du B.Y.O.D, le risque résulte principalement de l'intrusion frauduleuse au sein des systèmes d'information de l'entreprise. A ce titre, la jurisprudence a déjà jugé que « *l'accès frauduleux, au sens de la loi, vise tous les modes de pénétration irréguliers d'un STAD, que l'accédant travaille déjà sur la même machine mais à un autre système, qu'il procède à distance ou qu'il se branche sur une ligne de communication* »[74].

La notion d'«atteinte aux droits de la personne résultant des fichiers ou des traitements informatiques». Les articles 226-16 à 226-24 du Code pénal visent l'ensemble des infractions relatives à la violation des obligations prescrites par la loi Informatiques et Libertés n° 78-17 du 6 janvier 1978. La plupart d'entre elles sont sanctionnées de 5 ans d'emprisonnement et de 300.000 euros d'amende pour les personnes physiques.

L'utilisation d'équipements personnels par le salarié accroît d'une part, le risque de divulgation des données à caractère personnel à des tiers non autorisés (article 226-22 du Code pénal), et, d'autre part, le risque de manquement à l'obligation de sécuriser un traitement informatique comportant des données personnelles (article 226-17 du Code pénal).

En tout état de cause, la recherche de la responsabilité pénale de l'auteur du délit, de quelque nature que ce soit, n'exclut pas la présentation de demandes d'indemnisation en dommages et intérêts pour réparer le préjudice subi par l'entreprise.

CONCLUSION

Les risques encourus par le phénomène du B.Y.O.D. rappellent aux entreprises la nécessité d'organiser efficacement – en interne – la bonne gouvernance de leurs systèmes d'information, et en particulier des données traitées dans le cadre de leurs activités.

Des outils juridiques de protection, permettant d'encadrer l'accès et l'utilisation, par les salariés, du patrimoine informationnel de l'entreprise, doivent impérativement être mis en place en complément des mesures techniques. En cas de réalisation du risque, la sanction et la répression des comportements malveillants devra être organisée de façon stratégique au regard (i) de la nature des faits reprochés et (ii) du préjudice subi. La connaissance des aspects juridiques de la cybersécurité permettra à l'entreprise de sécuriser ses données stratégiques, de valoriser son capital, et d'accroître sa compétitivité.

[74] CA Paris, 5 avril 1994 ; CA Paris, 14 janvier 1997.

CHRISTINE GATEAU & OLIVIA BERNARDEAU-PAUPE[1]

L'impression 3D, révolution industrielle et juridique

CHRISTINE GATEAU, avocate associée, Hogan Lovells LLP, Paris

OLIVIA BERNARDEAU-PAUPE, avocate *counsel*, Hogan Lovells LLP, Paris

RÉSUMÉ

L'impression 3D, technologie existant depuis de nombreuses années, mais cantonnée jusqu'à présent au secteur industriel, se développe de manière fulgurante au point d'être à l'entrée de chacun de nos habitats. Dès demain, elle permettra aux consommateurs de reproduire, sans se déplacer de chez eux, les objets quotidiens. Du fait de ses applications sans limite, son impact futur sur l'économie est indiscutable. Mais qu'en est-il des risques liés à son utilisation ? Alors que le recours à l'imprimante 3D ne cesse de croître, se posent tant la question du régime de responsabilité applicable en cas de dommages résultant de son utilisation, que celle du respect des droits de propriété intellectuelle.

INTRODUCTION

A bien des égards, l'imprimante 3D représente une véritable révolution technologique, constituant un nouvel outil de conception et de production.

L'impression 3D consiste à scanner un objet, lequel sera alors reproduit avec une forme tridimensionnelle identique. Les matériaux, les couleurs et les dimensions utilisés pour la reproduction peuvent être variables et différer de ceux identiques à ceux composant l'objet d'origine.

Ce mode de production s'est considérablement développé. Ainsi, de nombreuses start-up proposent un service d'impression 3D en ligne permettant aux utilisateurs de générer et de convertir des objets numériques en objets tridimensionnels.

[1] Les auteurs remercient Marie Gayno et Sophie de Marez Oyens pour leur aide lors de la rédaction de cet article.

Après avoir scanné l'objet qu'il souhaite reproduire, l'utilisateur recourt à un logiciel 3D, lequel traite l'information et produit un fichier de conception assistée par ordinateur (communément appelé "CAO") contenant une image de synthèse en 3D. Ce fichier, souvent en format Standard Tessellation (STL), est alors transmis à la machine 3D, où un second logiciel réalise une découpe du modèle en plusieurs couches d'impression d'épaisseurs fixes. Les couches sont enfin empilées les unes sur les autres afin de réaliser le modèle. Ce mécanisme de fabrication par couches successives permet de matérialiser des objets comportant des cavités et des éléments imbriqués de dimensions et couleurs précises. L'imprimante 3D permettrait de fabriquer et produire des objets avec une précision encore jamais égalée.

Aujourd'hui, les utilisateurs de l'impression 3D sont essentiellement des professionnels qui utilisent l'imprimante 3D afin d'élaborer des prototypes ou de personnaliser des objets du quotidien. L'imprimante 3D permet, par exemple, de fabriquer des prothèses, de reproduire des coques de téléphone portable, des armes à feu, voire même des maisons. Accessible à tous, l'imprimante 3D peut aussi être utilisée par les consommateurs.

Prenons l'exemple d'un parent qui utiliserait son imprimante domestique afin de reproduire le jouet préféré de son enfant. Qui sera alors responsable si le jouet fabriqué n'est pas conforme aux normes de sécurité, si l'enfant fait une allergie aux matériaux utilisés, ou si le jouet est inflammable ? Le parent pourra-t-il chercher la responsabilité du fabricant de l'imprimante 3D, de son vendeur ou directement de l'entreprise ayant fabriqué le jouet initial ? Le parent, victime par ricochet, a-t-il une part de responsabilité, ayant fabriqué lui-même la pièce défectueuse ? Quid si un garagiste décide de remplacer une pièce défectueuse d'un véhicule par une pièce reproduite par impression 3D ? En cas d'accident, qui sera considéré responsable ? L'obligation d'information ou de sécurité pèse-t-elle sur le garagiste qui a vendu les pièces défectueuses, ou sur le constructeur de l'imprimante qui n'a pas suffisamment communiqué sur les risques liés aux pièces reproduites par impression 3D ?

Les acteurs susceptibles d'engager leur responsabilité sont nombreux : les créateurs de fichiers CAO, les éditeurs de logiciels, les plateformes et les sites de téléchargement, le fabricant et le vendeur de l'imprimante 3D, et le fournisseur du service d'impression.

Alors que son utilisation ne cesse de croître, se posent tant la question du régime de responsabilité applicable en cas de dommages résultant de son utilisation (**I**) que celle du respect des droits de propriété intellectuelle (**II**).

I. LA QUESTION DU RÉGIME DE RESPONSABILITÉ APPLICABLE EN CAS DE DOMMAGES RÉSULTANT DE L'UTILISATION DE L'IMPRESSION 3D

Outre le droit civil de la responsabilité qui sera abordé dans cet article, des actions pénales peuvent être engagées. Seront alors appliqués des délits de droit commun tels que la mise en danger d'autrui (article 121-3 du Code pénal), l'atteinte involontaire à l'intégrité de la personne (blessure, articles 222-19 et 222-20 du Code pénal ; ou même l'homicide involontaire, article 221-6 du Code pénal). Cela impliquerait alors, pour les sociétés, des amendes pouvant aller jusqu'à 225.000 euros, et pour les dirigeants, des peines pouvant aller

jusqu'à 45.000 euros d'amende ou jusqu'à trois ans d'emprisonnement. Comment appréhender le droit de la responsabilité du fait de produits fabriqués par des imprimantes 3D ? Les différents acteurs peuvent voir engager leur responsabilité au titre des obligations d'information, de sécurité et de notification (**A**). La victime pourrait aussi recourir à la responsabilité du fait des produits défectueux afin d'obtenir le dédommagement de son préjudice (**B**).

A. Responsabilité fondée sur des obligations de droit commun

Les acteurs de la production par imprimante 3D pourraient voir leur responsabilité engagée sur le terrain du droit commun, au titre d'obligations préventives d'information (**1**), et de sécurité (**2**). A titre palliatif, ils se voient aussi imposer une obligation de notification (**3**).

L'obligation d'information

Le professionnel est tenu de communiquer à l'autre partie les informations relatives à l'objet du contrat. Toutefois, l'étendue de l'obligation d'information variera en fonction des connaissances et de la qualité des parties en présence.

Le fabricant, le producteur et le vendeur, du fait de leur qualité professionnelle, sont tenus de communiquer les données nécessaires à leur contractant. Ils doivent informer leurs clients du mode d'emploi et des dangers des produits qu'ils fabriquent, produisent ou vendent. L'obligation est due, tant à l'égard d'un acheteur profane, que d'un acheteur professionnel, dans l'hypothèse où la compétence de ce dernier ne lui donne pas les moyens d'apprécier la portée exacte des caractéristiques de l'objet du contrat[2].

Il s'agit d'une obligation de résultat, pour ce qui est de l'existence même des informations à fournir. Toutefois, l'obligation reste de moyens, concernant la teneur et le contenu des informations fournies, ainsi que la compréhension de ces dernières par le bénéficiaire. L'obligation sera d'autant plus forte que le produit est dangereux ou nouveau[3].

En amont de la chaine de production par imprimante 3D, le fabricant d'imprimante 3D est tenu d'informer ses cocontractants sur le mode d'emploi de l'imprimante. Au titre de cette obligation d'information, il pourrait être tenu d'informer des dangers de la reproduction par imprimante 3D. Toutefois, dès lors que l'imprimante 3D permet de reproduire une quantité innombrable d'objets, le juge pourra difficilement imposer aux fabricants de fournir une information exhaustive.

La plate-forme d'intermédiation est, elle aussi, tenue d'informer ses internautes. Ayant connaissance de l'objet à reproduire, elle sera plus à même d'informer les consommateurs sur les matières pouvant être utilisées et sur l'utilisation pouvant être faite de l'objet reproduit à l'aide du fichier CAO.

Le vendeur dans le magasin spécialisé dans les imprimantes 3D est, quant à lui, en mesure de se renseigner sur le besoin exact de son client et sur l'usage qu'il compte faire de l'imprimante

[2] Cass. Civ. 1ère, 20 juin 1995, n° 93-15.948.
[3] Cass. Civ. 1ère, 11 octobre 1983, n° 82-13.633 ; Cass. Civ 3ème, 18 février 2004, n° 02-17.523.

3D. Il sera probablement tenu de délivrer des informations précises répondant aux besoins du client, de le conseiller sur l'usage de l'imprimante 3D.

Enfin, le vendeur de l'objet reproduit par imprimante 3D est, lui aussi, tenu d'une obligation d'information concernant ledit objet. Il convient de distinguer le vendeur occasionnel du vendeur professionnel et spécialisé. Le vendeur occasionnel n'est tenu de dire que ce qu'il sait. Ainsi, le vendeur occasionnel ne sera tenu de transmettre à son interlocuteur que les informations qu'il détient, notamment le fait même qu'il s'agit d'un objet reproduit par impression 3D. Au contraire, le professionnel spécialisé, devant avoir la maîtrise de la chose, est tenu de donner à l'acquéreur toutes les précisions indispensables ou utiles à l'usage de la chose vendue. Ainsi le professionnel, qui utilise une imprimante 3D pour produire les objets qu'il commercialise ensuite, sera tenu d'informer son client du mode d'emploi de l'objet reproduit et des dangers qui peuvent en émaner.

Le défaut ou le manque d'information peut engager la responsabilité contractuelle de son auteur, et la victime pourra obtenir la réparation de son dommage. Toutefois, le non-respect de l'obligation d'information ne pourra pas entrainer la nullité du contrat[4].

Si l'objet cause un dommage à un tiers, ce dernier peut lui aussi invoquer un manquement à l'obligation d'information sur le fondement de la responsabilité délictuelle, dès lors que ce manquement lui a causé un dommage[5]. Ainsi, le tiers qui obtient l'objet reproduit par imprimante 3D de l'acquéreur pourra toujours invoquer le défaut d'information pour engager la responsabilité d'un des acteurs professionnels. Il devra toutefois démontrer que l'insuffisance ou le défaut d'information est bien la cause du dommage subi.

Il est intéressant de noter que le législateur a consacré et codifié l'obligation d'information à l'égard du consommateur, tant à propos de l'obligation d'information du vendeur professionnel de biens meubles (article L. 111-1, III du Code de la consommation), que du professionnel prestataire de service (article L. 111-2, V du Code de la consommation).

L'obligation de sécurité

Au visa de l'article 1147 du Code civil, la jurisprudence a détaché de la garantie des vices cachés une obligation de sécurité autonome à la charge du vendeur professionnel et du fabricant. Le fabricant est ainsi tenu de livrer un produit exempt de tout défaut de nature à causer un danger pour les personnes ou les biens, c'est-à-dire un produit qui offre la sécurité à laquelle on peut légitimement s'attendre[6]. De même, le vendeur professionnel est tenu de livrer des produits exempts de tout vice ou de tout défaut de fabrication de nature à créer un danger pour les personnes ou les biens. Il est responsable tant à l'égard des tiers que de son acquéreur[7]. Cette obligation de sécurité a ensuite été étendue au producteur.

Cette obligation de moyens devient une obligation de résultat lorsque le client est un consommateur. En effet, l'article L. 221 du Code de la consommation dispose que « *les produits et les services doivent, dans des conditions normales d'utilisation ou dans d'autres*

[4] Cass. Civ. 1ère, 31 octobre 2007, n° 05-15.601.
[5] Cass. Ass. Plén., 6 octobre 2006, n° 05-13.255.
[6] Cass. Civ. 1ère, 3 mars 1998, n° 96-12.078.
[7] Cass. Civ. 1ère, 17 janvier 1995, n° 93-13.075.

conditions raisonnablement prévisibles par le professionnel, présenter la sécurité à laquelle on peut légitimement s'attendre et ne pas porter atteinte à la santé des personnes ». Pèse alors sur les professionnels une obligation de sécurité sans faute, en raison de la défectuosité du produit, dès lors que la preuve du rôle causal du produit dans la survenance du dommage est rapportée. A la différence de l'obligation jurisprudentielle, la violation de l'obligation légale d'information du consommateur peut entrainer des sanctions pénales ou frapper le contrat de nullité[8]. En outre, la jurisprudence a accepté la condamnation in solidum du fabricant et du vendeur d'un produit présentant un défaut de sécurité[9].

Le Code de la consommation ne fait pas de distinction entre les produits présentant un risque inhérent (comme les couteaux ou les armes à feu) et les autres produits. Au contraire, la Direction Générale Sécurité et Prévention (DGSP) n'exige pas que les biens soient totalement sans risque.

Ainsi, le vendeur et le fabricant de l'imprimante seraient tenus d'assurer que l'imprimante soit exempte de tout défaut de nature à causer un danger à autrui ou aux biens. Les éditeurs de logiciels seraient, quant à eux, tenus d'assurer l'absence de danger résultant de l'usage desdits logiciels. Les créateurs de fichiers CAO, ainsi que les plates-formes et sites de téléchargement, devraient prévenir tout danger pouvant résulter des fichiers CAO. Enfin, le vendeur, qui utilise une imprimante 3D pour fournir sa production serait, tenu d'assurer que les reproductions soient exemptes de tout vice pouvant causer un danger.

Un tiers, qui subit un dommage suite à l'usage d'un objet reproduit par impression 3D, peut-il rechercher la responsabilité délictuelle du fabricant ou du vendeur pour défaut de sécurité ? La Cour de cassation a déjà étendu l'obligation contractuelle de sécurité afin de l'appliquer au domaine délictuel. Ainsi, alors qu'un enfant s'était blessé dans une cour de récréation avec un objet appartenant à l'école, les juges de la Cour de cassation ont retenu la responsabilité délictuelle d'une société fabricante et distributrice. L'arrêt de la Cour de cassation rejetait alors le moyen fondé sur l'absence de faute délictuelle considérant que « *le vendeur professionnel est tenu de livrer des produits exempts de tout vice ou de tout défaut de fabrication de nature à créer un danger pour les personnes et les biens,* […] *il en est responsable tant à l'égard des tiers que de son acquéreur* ».

La responsabilité fondée sur l'obligation de sécurité couvre un champ largement étendu. Mais les juges iront-il jusqu'à engager la responsabilité du vendeur de l'imprimante 3D, du fabricant de l'imprimante 3D ou de l'éditeur du logiciel, pour défaut de sécurité, à la suite d'un préjudice résultant de l'usage d'une reproduction faite par l'imprimante (et non directement de l'usage de l'imprimante elle-même) ? C'est peu probable, car cela reviendrait à imposer au fabricant et vendeur d'imprimante 3D d'assurer la sécurité des objets créés par l'imprimante 3D, chose qu'ils ne peuvent pas réellement maîtriser.

L'obligation de notification et l'intervention de l'Etat

Le Code de la consommation impose une obligation de notification aux producteurs et aux distributeurs lorsque les produits mis sur le marché ne répondent pas aux exigences de

[8] Cass. Civ. 1ère, 7 décembre 2004.
[9] CA Douai, 7 janvier 1999.

sécurité de l'article L. 221-1. L'article L. 221-1-3 du Code de la consommation leur impose d'informer « *immédiatement les autorités administratives compétentes, en indiquant les actions qu'il engage afin de prévenir les risques pour les consommateurs* ».

Ainsi, des décrets en Conseil d'Etat peuvent intervenir afin de fixer par exemple des conditions de fabrication, d'importation, ou d'exportation. Ils peuvent aussi déterminer des conditions d'hygiène et de salubrité, ou ordonner le retrait du marché ou la destruction du produit.

L'article L. 221-5 du Code de la consommation prévoit qu'en cas de danger grave ou immédiat, l'autorité compétente puisse formuler des arrêtés de suspension de la fabrication, importation, exportation et mise sur le marché, ou des décrets d'interdiction[10]. Il peut également être ordonné la diffusion de mises en garde ou de précaution d'emploi, ainsi que le rappel en vue d'un échange, d'une modification ou d'un remboursement partiel ou total.

Enfin, l'autorité compétente est en mesure de demander aux fabricants, importateurs, distributeurs ou prestataires de service de mettre en conformité leurs produits conformément à l'article L. 221-7 du Code de la consommation.

Autant de mesures, qui, prisent en collaboration avec les autorités compétentes, permettront de sécuriser l'usage des imprimantes 3D et d'intervenir à titre préventif ou palliatif afin de limiter le risque de responsabilité de ses acteurs.

La victime pourra, en parallèle des actions en responsabilité précitées, agir sur le fondement de la responsabilité du fait des produits défectueux des articles 1386-1 et suivants du Code civil.

B. La responsabilité du fait des produits défectueux

A titre délictuel, l'article 1386-1 du Code civil dispose que « *le producteur est responsable du dommage causé par un défaut de son produit, qu'il soit ou non lié par un contrat avec la victime* ». L'article 1386-4 du Code civil ajoute qu' « *un produit est défectueux au sens du présent titre lorsqu'il n'offre pas la sécurité à laquelle on peut légitimement s'attendre* ». Afin d'apprécier la défectuosité du produit, il faudra notamment tenir compte de la présentation du produit, de l'usage qui peut en être raisonnablement attendu et du moment de sa mise en circulation.

S'agissant d'une responsabilité sans faute, l'article 1386-9 du Code civil dispose que la victime doit seulement démontrer un dommage, un défaut du produit et un lien de causalité entre ce défaut et le dommage.

Appliqué aux dommages résultants d'objets imprimés en 3D, il faut s'intéresser au lien de causalité pour déterminer à quels acteurs peut s'appliquer le régime de la responsabilité du fait des produits défectueux.

[10] Article L. 221-5 du Code de la consommation.

S'agissant d'abord du producteur ou du distributeur d'imprimante 3D, il faudra caractériser un lien de causalité entre l'imprimante elle-même et le dommage résultant de l'usage de l'objet reproduit. La victime devra alors démontrer que le dommage a été causé par le défaut de l'imprimante, laquelle ne présentait pas la sécurité à laquelle on pouvait légitimement s'attendre.

Il en est de même du producteur et du distributeur de la matière utilisée pour la reproduction par imprimante 3D. Le lien de causalité semble plus évident dès lors que l'on peut imaginer un dommage causé directement du fait de la matière utilisée pour la reproduction de l'objet, matière ayant des propriétés différentes de celles du produit d'origine.

Par ailleurs, les créateurs de fichiers CAO ou les éditeurs de logiciels CAO pourraient voir leur responsabilité engagée au visa des articles 1386-1 et suivant du Code civil du fait d'un défaut du fichier CAO contenant une image de synthèse en 3D, lequel présenterait un défaut de sécurité ayant causé le dommage.

L'action en responsabilité du fait des produits défectueux est prescrite après trois ans à compter de la date où la victime a eu connaissance du dommage, du défaut et de l'identité du fabricant.

La victime pourra obtenir des dommages et intérêts équivalents à la perte causée par le produit défectueux. En revanche, elle n'obtiendra pas de réparation pour le dommage affectant le produit défectueux lui-même.

Conformément à l'article 1386-18 du Code civil, l'action en responsabilité du fait des produits défectueux peut être cumulée avec des actions en responsabilité contractuelle ou délictuelle de droit commun. Ainsi, la victime pourra assortir son action en responsabilité du fait des produits défectueux d'une action en responsabilité contractuelle ou délictuelle fondée sur le défaut d'information ou sur le défaut de sécurité.

Alors que l'impression 3D ouvre de nombreuses perspectives économiques et pourrait influencer les modes de production de nombreux secteurs, le régime de responsabilité préexistant semble largement applicable. Afin d'éviter de voir leur responsabilité engagée, les différents acteurs et usagers devront donc veiller à respecter leurs différentes obligations. Ils devront anticiper et prévenir les risques pouvant résulter de l'usage de l'imprimante 3D. En cas de débordement, la jurisprudence future se chargera quant à elle d'appliquer à cette nouvelle technologie les outils fournis par le droit de la responsabilité.

Outre les problématiques liées à la responsabilité des différents acteurs de l'impression 3D fondée sur les obligations de droit commun, et à la responsabilité du fait des produits défectueux, il convient de discuter des implications de cette technique sur le droit de la propriété intellectuelle.

Impression 3D et droit de la propriété intellectuelle

En ce qu'elle bouleverse les réseaux traditionnels de distribution et permet aisément la reproduction ou la modification d'objets existants, l'impression 3D engendre notamment de nouvelles questions de droit d'auteur sur les objets qu'elle permet de reproduire.

La révolution à venir en termes d'atteinte au droit d'auteur concerne principalement la copie privée d'objets réalisée par des consommateurs[11]. C'est essentiellement l'échelle de la reproduction privée de fichiers d'objets numériques et d'objets 3D eux-mêmes, entraînant potentiellement une contrefaçon de masse, qui inquiète les titulaires de droits. Il s'agit donc d'examiner la protection par le droit d'auteur des « *œuvres* » nouvelles, à savoir les fichiers CAO et les objets finaux, imprimés en 3D (**A**), puis la contrefaçon du droit d'auteur par l'impression 3D, ainsi que l'exception pour copie privée et son application potentielle au cas de l'impression 3D d'un objet protégé (**B**), avant d'aborder les responsabilités spécifiques des différents acteurs de la chaîne d'impression (**C**). Des pistes de réflexion pour trouver des solutions pragmatiques seront abordées en conclusion de cet article.

A. De nouvelles créations dignes de protection ?

Les consommateurs peuvent adopter un rôle créatif lors de l'impression de leur objet en 3D. En effet, l'impression 3D permet la réplique d'un objet existant mais également sa personnalisation. Le consommateur devient alors un « *prosommateur* », un mélange entre un « *consommateur* » et un « *producteur* »[12]. Ainsi il a été estimé que « *l'impression 3D marque* […] *une nouvelle ère de personnalisation en masse qui promet de stimuler l'innovation, d'encourager une meilleure utilisation des ressources et de transformer la façon de fabriquer des objets* »[13]. L'impression 3D permettrait un nouveau « remix » d'objets numériques et physiques[14]. Outre la personnalisation d'un objet existant, l'impression 3D peut également encourager les créations entièrement nouvelles.

Puisque l'article L. 112-1 du Code de la propriété intellectuelle (CPI) protège « *les droits des auteurs sur toutes les œuvres de l'esprit* », la question se pose de la protection par le droit d'auteur tant du fichier CAO contenant l'objet sous forme numérique (**1**) que de l'objet final en trois dimensions (**2**).

1. Le fichier CAO

Le fichier CAO, nécessaire à l'impression de l'objet final en 3D, peut être obtenu, soit en scannant un objet à l'aide d'un scanner 3D, soit en utilisant un logiciel de modélisation 3D. Il a été soutenu que la numérisation d'une œuvre présenterait cependant moins d'implication créative que la création d'un fichier CAO à l'aide d'un logiciel de modélisation. Ceci n'écarte cependant pas nécessairement la protection du fichier créé à l'aide d'un scanner si l'on se rapporte à la position de la jurisprudence en ce qui concerne les photographies, auxquelles une protection par le droit d'auteur est accordée[15]. Tant la Cour de Justice de l'Union

[11] G. COURTOIS, « *Pourquoi l'impression 3D va bouleverser la propriété industrielle* », Les Echos, 11 février 2014.
[12] P. LI, S. MELLOR, J. GRIFFIN, C. WAELDE, L. HAO et R. EVERSON, « *Intellectual property and 3D printing: a case study on 3D chocolate printing* », Journal of Intellectual Property Law & Practice 2014, vol. 9, n. 4, p. 323 : les auteurs utilisent le terme de "*prosumer*", un mélange entre "*consumer*" et "*producer*".
[13] C. JEWELL, « *L'impression 3D et le future des objets* », OMPI magazine juin 2013, http://www.wipo.int/wipo_magazine/fr/2013/02/article_0004.html.
[14] M. WEINBERG, « *It will be something awesome if they don't screw it up: 3D printing, intellectual property and the fight over the next great disruptive technology* », Public Knowledge novembre 2010, https://www.publicknowledge.org/news-blog/blogs/it-will-be-awesome-if-they-dont-screw-it-up-3d-printing.
[15] C. LE GOFFIC et A. VIVÈS-ALBERTINI, « *L'impression 3D et les droits de propriété intellectuelle* », Propriétés Intellectuelles, janvier 2014, n°50, p. 27-28.

Européenne (CJUE)[16], que les tribunaux français, adoptent une appréciation large du critère d'originalité. Dans les deux cas, il convient de démontrer l'originalité du fichier, à savoir vérifier qu'il porte l'empreinte de la personnalité de son auteur.

2. Les objets physiques eux-mêmes

Par ricochet, l'objet imprimé en 3D fera l'objet d'une protection par le droit d'auteur si le fichier CAO est protégé[17]. Son auteur est celui qui a créé le fichier CAO. L'acte d'impression à partir du fichier ne devrait pas conférer de droit d'auteur à l'utilisateur de l'imprimante qui ne peut effectuer de choix libres et créatifs, laissant l'empreinte de sa personnalité à l'objet imprimé.

En sa qualité de titulaire d'un droit d'auteur, le créateur d'une œuvre 3D peut donc refuser ou autoriser toute reproduction numérique ou physique de son œuvre.

B. Les atteintes au droit d'auteur et l'applicabilité douteuse de l'exception pour copie privée

L'impression 3D, qui permet la reproduction physique de fichiers numériques, annonce une nouvelle ère de contrefaçon du droit d'auteur (**1**). L'applicabilité de l'exception pour copie privée lorsque la copie de l'œuvre originale en 3D est réalisée à partir d'une source licite et à usage privé est certainement le point d'intérêt central pour les titulaires de droits (**2**).

1. Les atteintes au droit d'auteur

La contrefaçon numérique du droit d'auteur a désormais un impact plus direct sur le monde physique[18]. L'impression 3D d'un objet protégé par le droit d'auteur est susceptible de porter atteinte tant aux droits moraux de l'auteur (**a**) qu'à ses droits patrimoniaux (**b**).

a. Droits moraux

L'article L.121-1 du CPI reconnaît à l'auteur un droit à la paternité sur son œuvre, ainsi que le droit au respect de l'intégrité de son œuvre.

En ce qui concerne l'atteinte à la paternité de l'œuvre, elle sera vraisemblablement systématiquement constituée, à moins que le nom de l'auteur ne soit mentionné à la fois sur l'objet lui-même et sur le fichier CAO.

L'atteinte à l'intégrité de l'œuvre peut être caractérisée lors de l'impression d'un objet protégé en 3D. En effet, l'auteur peut s'opposer à l'altération, la dénaturation et la déformation de son œuvre. Si l'objet final est de moins bonne qualité que l'œuvre originale, l'atteinte peut être constituée. Il en va de même si les mesures de sécurité règlementaires n'ont pas été respectées.

---

[16] CJUE, arrêt *Painer c/ A. Springer et al,* C-145/10, 1er décembre 2011.

[17] C. LE GOFFIC et A. VIVÈS-ALBERTINI, art. cit., p. 29 ; G. COURTOIS, « *L'impression 3D : chronique d'une révolution juridique annoncée* », Revue Lamy Droit de l'Immatériel, 2013.

[18] B. RIDEOUT, « *Printing the impossible triangle: the copyright implications of three-dimensional printing* », Business, Entrepreneurship and the Law, vol. V.I, 2011, p. 161.

En outre, on pourrait envisager que le changement de matériau ou le changement de mesures par l'impression 3D de la copie porte atteinte à l'intégrité de l'œuvre originale. En effet, il a été jugé qu'une reproduction qui n'est pas fidèle à l'œuvre originale, du fait, notamment, d'une distorsion dans les mesures, constitue une contrefaçon de l'œuvre portant atteinte à son intégrité[19]. Il convient de souligner que la Cour de cassation adopte une jurisprudence très protectrice du droit à l'intégrité de l'œuvre, jugeant que toute modification porte atteinte à ce droit[20].

Aux côtés des droits moraux de l'auteur, l'impression 3D peut également porter atteinte aux droits patrimoniaux de celui-ci.

b. Droits patrimoniaux

L'impression 3D, au sens large, est susceptible de porter atteinte aux droits patrimoniaux de l'auteur reconnus à l'article L. 122-1 du CPI, à savoir, le droit de reproduction et le droit de représentation.

Le premier est défini comme « *la fixation matérielle de l'œuvre par tous procédés qui permettent de la communiquer au public d'une manière indirecte* » (L. 122-3 al. 1er du CPI) et le second « *consiste dans la communication de l'œuvre au public par un procédé quelconque* » (L. 122-2 al. 1er du CPI).

Ces droits sont susceptibles d'atteintes lors des différentes étapes du processus d'impression 3D. En effet, la numérisation de l'objet protégé met en cause le droit de reproduction, tout comme l'impression finale. Le droit de représentation, quant à lui, est susceptible d'atteinte au stade du partage du fichier CAO contenant l'œuvre protégée ou de la communication par tout moyen de l'objet 3D final.

Cependant, on peut s'interroger sur les limites de ces atteintes aux droits patrimoniaux, notamment par l'intermédiaire de l'exception pour copie privée qui permettrait au consommateur, sous certaines conditions, de reproduire en toute légalité des œuvres protégées par le droit d'auteur.

2. L'exception pour copie privée applicable à l'impression 3D ?

L'article L. 122-5 2° du CPI dispose que l'auteur ne peut interdire « *les copies ou reproductions réalisées à partir d'une source licite et strictement réservées à l'usage privé du copiste et non destinées à une utilisation collective, à l'exception des copies des œuvres d'art destinées à être utilisées pour des fins identiques à celles pour lesquelles l'œuvre originale a été créée* ».

Ainsi, pour que cette disposition puisse s'appliquer et que le copiste échappe à la qualification de contrefacteur, ce dernier ne peut copier l'œuvre protégée que pour un usage privé et non collectif. Cette condition exclut donc que cette disposition s'applique aux personnes morales, y inclus les sociétés proposant des services d'impression 3D à la demande.

[19] CA Paris, 16 novembre 2012, n°11/23303.
[20] Civ. 1ère, 5 décembre 2006, n°05-11.789.

En outre, les reproductions doivent être réalisées à partir d'une « *source licite* », ce qui inclut les objets achetés légalement par le copiste et exclut, a contrario, toute impression effectuée à partir d'un fichier contrefaisant téléchargé.

Il convient de noter que l'article L. 122-5 2° du CPI exclut l'application de l'exception à la copie des œuvres d'art protégées pour la même destination. Les contours de cette disposition – qui n'a pas trouvé une grande application à ce jour – devront être déterminés par la jurisprudence ou le législateur, puisqu'il subsiste un flou quant à la définition d' « *œuvre d'art* ».

Le véritable point épineux de l'application de cette exception à la contrefaçon par impression 3D se situe dans le « triple test » prévu à l'avant dernier alinéa du même article. En effet, même si les conditions de l'exception sont remplies, il convient d'examiner si l'exception, dans ce cas la copie privée, passe le test en l'espèce.

La première étape est la limitation des exceptions à des « *cas spéciaux* ». Cette limite peut paraître redondante puisque la liste des exceptions facultatives de l'article 5 de la directive 2001[21] est stricte et ne comprend donc que des « *cas spéciaux* ». Cette limitation vise à éviter les exceptions trop généralisées, ce qui n'est pas le cas en l'espèce, puisque les exceptions reconnues par le législateur français sont limitées et énumérées de manière exhaustive par le CPI.

La seconde limite concerne l'absence d'atteinte à l'exploitation normale de l'œuvre. L'exception pour copie privée ne doit pas, dans le cas d'espèce, porter une telle atteinte. Dans un rapport du 15 juin 2000, le panel de l'Organisation Mondiale du Commerce a estimé « *qu'une exception ou limitation concernant un droit exclusif* […] *va jusqu'à porter atteinte à l'exploitation normale de l'œuvre* […] *si des utilisations, qui en principe sont visées par ce droit mais bénéficient de l'exception ou de la limitation, constituent une concurrence aux moyens économiques dont les détenteurs du droit tirent normalement une valeur économique sur l'œuvre* (c'est-à-dire le droit d'auteur) *et les privent de gains commerciaux significatifs ou tangibles* »[22].

Au vu de cette définition, il apparaîtrait ici que la possibilité d'imprimer en 3D de manière illimitée et dans une qualité qui est – ou sera dans un futur proche – quasi-parfaite est susceptible de porter atteinte à l'exploitation normale de l'œuvre en ce qu'elle privera les auteurs et leurs ayants droits de gains commerciaux significatifs. Cette situation se distingue, en effet, de la copie de fichiers musicaux ou audiovisuels numériques, pour lesquels un particulier n'aurait que peu d'intérêt à copier en une multitude d'exemplaires. Il parait plus juste de dresser un parallèle avec la situation du logiciel, pour lequel il y a une réelle utilité à copier de multiples fois, puisque l'on peut utiliser les logiciels à des fins diverses. En effet, on pourrait imaginer que des consommateurs souhaitent imprimer en de multiples exemplaires certains objets de la vie quotidienne, protégés par le droit d'auteur. La copie privée a été exclue pour le logiciel et la reproduction a été limitée à un exemplaire de sauvegarde.

[21] Directive 2001/29/CE du Parlement européen et du Conseil du 22 mai 2001 sur l'harmonisation de certains aspects du droit d'auteur et des droits voisins dans la société de l'information.
[22] Rapport du Groupe spécial de l'Organisation Mondial du Commerce WT/DS160/R du 15 juin 2000, pt. 6.183.

Au regard de la limite concernant l'exploitation normale de l'œuvre, il semble probable que pour les mêmes raisons appliquées aux logiciels, la copie privée ne puisse trouver à s'appliquer à l'impression 3D à usage privé. On pourrait cependant imaginer une transposition de la solution posée à l'égard des logiciels en ce qui concerne la copie de sauvegarde au cas de l'impression 3D[23]. L'impression 3D privée pourrait se voir autorisée pour une seule copie, ce qui en pratique viderait de son intérêt l'acquisition d'une imprimante 3D.

La troisième et dernière limite concerne l'absence de préjudice injustifié aux intérêts légitimes de l'auteur. Selon le rapport précité, « *un préjudice causé aux intérêts légitimes des détenteurs atteint un niveau injustifié si une exception ou limitation engendre ou risque d'engendrer un manque à gagner injustifié pour le titulaire du droit d'auteur* »[24]. Cette définition adopte une analyse exclusivement économique des intérêts légitimes des auteurs.

Dans un tel cas, une licence obligatoire assortie d'un droit à compensation permet d'effacer le caractère « *injustifié* » du préjudice. La France a notamment mis en place un tel système pour compenser le préjudice du fait de la copie privée, appelé « *rémunération pour copie privée* »[25].

La rédaction de l'article L. 311-4 du CPI permet cependant de douter de l'applicabilité de ce système à l'impression numérique. En effet, cette disposition prévoit que la rémunération versée provient des « *supports d'enregistrement utilisables pour la reproduction à usage privé d'œuvres* ». Ainsi, les CD vierges, les clés USB, les disques durs externes et d'autres supports se voient appliquer une taxe, gérée par une société de gestion collective, et destinée à pallier le manque à gagner des auteurs. La liste des supports est déterminée par une commission spéciale, comme mentionné à l'article L. 311-5 du CPI. Or, l'imprimante 3D n'est pas un support mais un matériel nécessaire à la réalisation de l'impression. Ainsi, la terminologie des articles du CPI relatifs à la rémunération pour copie privée ne permet pas de les appliquer tels quels à l'impression 3D. Des pistes ont été évoquées, telle que la taxation de l'imprimante, du scanner 3D ou du disque dur de l'ordinateur permettant de créer le fichier CAO[26].

A ce stade, une intervention du législateur parait nécessaire afin de modifier la liste de l'article L. 311-5 du CPI.

Une décision de la CJUE du 27 juin 2013[27] laisserait envisager une certaine ouverture dans ce sens. Selon la Cour, il est possible pour les Etats de remonter aux étapes antérieures à la réalisation même de la copie et d'instaurer, aux fins du financement de la compensation équitable, une « *redevance pour copie privée* » à la charge des personnes qui disposent d'équipements, d'appareils et de supports de reproduction.

Une résolution a, en outre, été adoptée le 27 février 2014 par le Parlement européen sur les redevances pour copie privée[28]. Elle souligne la nécessité « *d'actualiser le mécanisme de copie*

[23] G. COURTOIS, « *L'impression 3D : chronique d'une révolution juridique annoncée* », art. cit.
[24] Rapport précité, point 6.229.
[25] Article L. 311-1 et s. du CPI.
[26] G. COURTOIS, « *L'impression 3D : chronique d'une révolution juridique annoncée* », art. cit.
[27] CJUE, arrêt *VG WORT*, C-457/11 à C-460/11, 27 juin 2013.
[28] Résolution du Parlement Européen sur les redevances pour copie privée du 27 février 2014, http://www.europarl.europa.eu/sides/getDoc.do?type=TA&reference=P7-TA-2014-0179&language=FR&ring=A7-2014-0114.

privée, en le rendant plus efficace et en tenant mieux compte de l'évolution technologique »[29] en trouvant « *un modèle plus efficace et plus moderne qui ne soit pas obligatoirement fondé sur une redevance forfaitaire liée aux appareils* »[30]. Elle souligne en effet « *les fortes disparités entre les systèmes nationaux de prélèvement des redevances, en particulier en ce qui concerne les types de produits soumis à redevance et le niveau de ces redevances* »[31]. Elle estime enfin que « *la redevance pour copie privée doit s'appliquer à tout matériel et support utilisé pour ses capacités d'enregistrement et de stockage d'œuvres à des fins privées lorsque les actes de copie privée entraînent un préjudice pour les créateurs* »[32].

On peut, enfin, se demander si les imprimeurs 3D pourront se prévaloir de l'exception pour copie privée dans d'autres pays de l'Union Européenne, contrairement à la France. En effet, et même si l'article 5.5 de la directive de 2001[33] prévoit le « *triple test* », il a été soutenu, par certains auteurs[34], que ce « *triple test* » n'était adressé qu'aux législateurs des Etats membres pour l'adoption des exceptions et non aux juges nationaux. Ainsi, l'Allemagne, la Belgique et les Pays-Bas, notamment, n'ont pas estimé nécessaire de le transposer dans leur législation. Bien que le juge soit tenu d'appliquer la loi en conformité avec le droit communautaire, l'absence du triple test dans la législation pourrait l'inciter à appliquer l'exception pour copie privée plus facilement au cas des impressions 3D.

La question se pose alors de savoir, parmi les différents acteurs de la chaîne de production d'une copie par impression 3D, quels sont ceux susceptibles de voir leur responsabilité engagée du fait de l'atteinte aux droits de propriété intellectuelle des titulaires.

C. La responsabilité des différents acteurs

En pratique, les titulaires de droits seront enclins à engager la responsabilité des acteurs commerciaux en priorité, tels que les sites offrant le téléchargement de fichiers CAO contenant des reproductions numériques contrefaisantes d'objets protégés ou des sociétés proposant d'imprimer des objets contrefaisants. Les actes de contrefaçon de ces derniers seront plus facilement repérables que ceux de l'utilisateur final et leur solvabilité est plus probable. Il convient de dresser un parallèle avec la situation en matière de téléchargement de fichiers musicaux et audiovisuels contrefaisants. Bien que la loi « Hadopi »[35] permette de poursuivre les utilisateurs finaux, très peu de dossiers de « *contrefacteurs* » ont en réalité été transmis à la justice[36]. Ceci marque un fort contraste avec la multiplication des actions à l'encontre des plateformes de téléchargement et de streaming proposant des contenus

[29] *Idem*, pt. E.
[30] *Idem*, pt. J.
[31] *Idem*, pt. 7.
[32] *Idem*, pt. 9.
[33] Directive 2001/29/CE du Parlement européen et du Conseil du 22 mai 2001 sur l'harmonisation de certains aspects du droit d'auteur et des droits voisins dans la société de l'information.
[34] Notamment, M. Senftleben, « *Copyright, Limitations and the Three-Step Test* », Information Law Series 13, 2004.
[35] Loi n° 2009-669 du 12 juin 2009 favorisant la diffusion et la protection de la création sur internet, dite "loi Hadopi".
[36] J. COHENDET et V. DUNATE, « *Hadopi: un internaute sur 10 a déjà reçu un mail d'avertissement* », France Info, 17 juillet 2014, http://www.franceinfo.fr/vie-quotidienne/high-tech/article/hadopi-un-internaute-sur-10-deja-recu-un-mail-d-avertissement-534819.

contrefaisants. Qu'en est-il des différents acteurs du processus d'impression 3D, du créateur du fichier CAO au fournisseur du service d'impression ?

1. Le créateur du fichier CAO

Le créateur du fichier CAO est celui qui numérise un objet existant grâce à un scanner 3D ou qui créé le fichier grâce à un logiciel d'images de synthèse. Il sera contrefacteur s'il y a reproduction d'un objet protégé par le droit d'auteur, sans autorisation du titulaire des droits et dans un cadre dépassant le strict usage privé (si on estime que l'exception pour copie privée s'applique dans ce cadre).

2. L'éditeur du logiciel CAO

Est contrefacteur et peut être sanctionné pénalement sur le fondement de l'article L. 335-2-1, 1° du CPI « *le créateur d'un logiciel qui édite, met à la disposition du public ou communique au public, sciemment et sous quelque forme que ce soit, un logiciel manifestement destiné à la mise à disposition du public non autorisée d'œuvres ou d'objets protégés* ». Le logiciel CAO a pour fonction de permettre la création de fichiers CAO afin de rendre possible l'impression en 3D d'un objet. Or, tous les objets présents dans les fichiers CAO et imprimés en 3D ne sont pas soumis à la protection par le droit d'auteur. Ces logiciels ne sont pas « *manifestement destinés à la mise à disposition du public non autorisée d'œuvre ou d'objets protégés* » et leurs créateurs devraient échapper à toute sanction sur ce fondement.

3. L'hébergeur de site de téléchargement de fichiers CAO : une responsabilité aménagée

L'hébergeur d'un site internet est un prestataire technique qui stocke et transmet des informations sur son site. Il bénéficie, au titre de l'article 6 de la loi pour la confiance dans l'économie numérique[37], d'une responsabilité « *aménagée* ». Ainsi, l'hébergeur du site internet proposant des fichiers CAO à télécharger ne sera responsable du contenu contrefaisant, présent sur le site qu'il héberge, que s'il a connaissance du caractère illicite des fichiers, ou s'il ne supprime pas promptement le contenu manifestement illicite qui lui est notifié, en application de la procédure prévue par cette loi.

4. L'éditeur de site de téléchargement de fichiers CAO

L'éditeur d'un site internet, au contraire de l'hébergeur, est celui qui créé le site et en fournit surtout le contenu. Il est responsable de ce contenu, et sera contrefacteur, si les fichiers CAO fournis sans autorisation sont protégés par un droit d'auteur.

La question de la qualification d'hébergeur ou d'éditeur d'une plateforme de téléchargement de fichiers CAO se pose de la même manière qu'elle s'est posée en matière de fichiers musicaux et audiovisuels contrefaisants. On peut déjà en voir une illustration avec le fameux site de bit torrent « *The Pirate Bay* » qui a ouvert une section « *physibles* », afin que les internautes puissent mettre à disposition des liens de téléchargement vers des fichiers CAO[38].

[37] Loi n° 2004-575 du 21 juin 2004.
[38] K. SCOTT, « *The Pirate Bay adds 'physibles' 3D-printing category* », Wired, 24 janvier 2012, http://www.wired.co.uk/news/archive/2012-01/24/pirate-bay-introduces-physibles.

5. Le fabricant et fournisseur de matériel d'impression

Les fabricants et fournisseurs de matériel d'impression ne sont pas susceptibles de voir leur responsabilité engagée au titre de la contrefaçon de droit d'auteur sur une œuvre reproduite par impression 3D. En effet, pour être jugés complices d'un délit de contrefaçon, ils doivent avoir connaissance de l'usage illégal de leurs appareils. Or, ils se retrouvent ici dans la même situation que les fabricants d'imprimantes traditionnelles, d'ordinateurs ou de graveurs, autant d'acteurs dont la responsabilité ne se trouve bien heureusement pas engagée aujourd'hui.

6. Le fournisseur de service d'impression

D'après la célèbre décision de la Cour de cassation, *Ranou-Graphie*[39], a été considérée comme copiste l'officine de photocopie qui « *détenant dans ses locaux, le matériel nécessaire à la confection de photocopies, exploite ce matériel en le mettant à la disposition de ses clients* ». La personne qui met à la disposition du public les moyens de reproduire des œuvres doit donc *a priori* être considérée comme copiste. Le fournisseur d'un service d'impression 3D pourra donc voir sa responsabilité pour contrefaçon engagée s'il réalise l'impression non autorisée d'objets protégés ou permet un libre-service de ses machines. Bien que des décisions rejettent l'argument tiré de l'exclusion de responsabilité par la société de reprographie[40], les sociétés proposant des services d'impression 3D à la demande pourraient avoir un intérêt à inclure une telle exclusion dans leurs conditions générales d'impression.

CONCLUSION : UNE ADAPTATION NÉCESSAIRE DU BUSINESS MODÈLE DE FABRICANTS ET TITULAIRES DE DROITS – ATTENTION À NE PAS RATER LE COCHE !

Les outils juridiques, technologiquement neutres, continuent à protéger les auteurs contre les actes de contrefaçon, y compris dans le cas d'impressions 3D contrefaisantes. Cependant, de multiples doutes subsistent et une précision législative s'avère nécessaire, notamment quant à l'application de l'exception pour copie privée à l'impression 3D contrefaisante.

Il est important que les titulaires de droits d'auteur tirent des leçons de l'échec supporté par l'industrie de la musique et du cinéma, dont la résistance opposée à l'apparition de nouveaux supports et modes de diffusion s'est avérée vaine. Ces industries auraient tout à gagner à réfléchir aux nouvelles possibilités commerciales que propose l'impression 3D. En investissant ce nouveau marché dès à présent, les titulaires de droits pourront apercevoir les bénéfices de cette nouvelle technologie et non seulement le manque à gagner dû à la contrefaçon. En se bornant à combattre cette « *révolution* », en revanche, ils risqueraient, comme en matière de téléchargement de fichiers musicaux ou audiovisuels, d'encourager la contrefaçon.

Un auteur met en avant l'idée du « *one-stop shop* », sur le modèle d'Itunes, où les auteurs pourraient vendre les matériaux nécessaire à l'impression d'objets en 3D, ce qui leur assurerait un revenu, sans qu'ils aient à supporter les coûts liés à la production des objets en eux-mêmes,

[39] Cass. Civ. 1ère, 7 mars 1984, n° 82-17.016, *Ranou-Graphie*.
[40] CA Paris, 25 juin 1997, Juris-Data n° 023142, *Société Reproprint / Société centre français d'exploitation du droit de copie*.

en termes de main d'œuvre, de transport et de stockage[41]. De nouvelles sociétés pourront être créées dont l'unique activité serait de vendre des fichiers CAO destinés à permettre une impression 3D maison, en accord avec les auteurs qui concluront des contrats de licence sur la vente de fichiers CAO contenant leur création, laissant la possibilité aux utilisateurs finaux d'imprimer les objets protégés dans un cadre contractuel défini – en termes de qualité, de quantité et de durée par exemple. Les sociétés qui proposent déjà les biens physiques protégés – et qui bénéficient de contrats de licence ou de distribution – pourront s'adjoindre un service de fichiers numériques[42]. Ces derniers seraient alors proposés à un prix compétitif par rapport à leur équivalent « *pré-fabriqué* ».

Des mesures de protection techniques pourraient également être liées à ces fichiers (articles L. 331-5 et L. 331-11 du CPI). A cet égard, un brevet « *système de contrôle de fabrication* » a été déposé aux Etats-Unis en 2012 par la société Intellectual Ventures, dirigée par l'ancien directeur technique de Microsoft. Il permet de contrôler les impressions d'objets contenus dans des fichiers CAO, avec la création d'une base de données, dans laquelle les titulaires de droits pourraient enregistrer leurs créations. Le brevet prévoit que l'utilisateur ayant installé le fichier CAO, lui-même contenant l'objet à imprimer sous forme numérique, l'imprimante vérifiera alors dans la base de données les droits attachés à cet objet et les modalités d'impression autorisées (à savoir, les matériaux, le nombre d'impressions autorisées, etc.)[43].

Une telle base de données pose néanmoins de nombreux problèmes pratiques, tels que son caractère obligatoire pour des œuvres qui ne seraient pas nécessairement originales. A ce jour, il n'y a pas de réponse satisfaisante.

Ces ébauches de solutions ne pourront, dans tous les cas, être mises en œuvre que si les sociétés d'intermédiaires adoptent une attitude responsable vis-à-vis des titulaires de droits. Qu'il s'agisse des plateformes de téléchargement en ligne de fichiers, des sociétés de fabrication des imprimantes, ou des sociétés de services d'impression à la demande, leur coopération sera essentielle.

[41] Dr. D. MENDIS, « *"The clone wars": episode 1 – The rise of 3D printing and its implications for intellectual property law – learning lessons from the past?* », European Intellectual Property Review, 2013.
[42] V. ARÈNE, « *Créer sa coque de Lumia 820 avec une imprimante 3D* », Le Monde Informatique, 18 janvier 2003 : Nokia a mis à disposition de ses clients des fichiers CAO permettant d'imprimer sur n'importe quelle imprimante 3D, le modèle d'un de ses étuis pour téléphone mobile, http://www.lemondeinformatique.fr/actualites/lire-creer-sa-coque-delumia-820-avec-une-imprimante-3d-52132.html.
[43] A. REGALADO, « *Nathan Myhrvold's cunning plan to prevent 3-D printer piracy* », MIT Technology Review, 11 octobre 2012.

ANNE-LAURE VILLEDIEU & JULIE TAMBA

Le droit, protecteur des données dans le Cloud

ANNE-LAURE VILLEDIEU, avocate associée, CMS Bureau Francis Lefebvre

JULIE TAMBA, avocate, CMS Bureau Francis Lefebvre

RÉSUMÉ

Si le Cloud computing rend possible une mutualisation des ressources entre les utilisateurs, permettant de réduire, en les divisant, les coûts de maintenance, d'exploitation, de matériel et d'énergie, le partage des données qui en procède suscite de nouveaux enjeux et risques. Tour d'horizon des précautions nécessaires lors de la conclusion d'un contrat avec un prestataire Cloud.

INTRODUCTION

A l'heure où les photographies de Jennifer Lawrence piratées sur l'iCloud font l'actualité sur le Web et que le moteur de recherche Yahoo ! confirme, preuves à l'appui[1], avoir été contraint de communiquer les données de ses utilisateurs à la National Security Agency (NSA), il semble opportun de se pencher sur les problématiques relatives aux services de Cloud Computing.

Le Cloud Computing a fait exploser l'offre informatique « *As A Service* » (aaS), c'est-à-dire externalisée et accessible à distance par le biais d'internet. Particuliers et professionnels utilisent désormais largement, et parfois même sans en avoir conscience, ce genre de service. L'offre informatique « *As A Service* » consiste classiquement à offrir aux internautes de simples services de stockage, d'hébergement ou de sauvegarde, également désignés « *Infrastructure As A Service* » (IaaS), de logiciels systèmes dits « *Platform As A Service* » (PaaS), ou encore d'applications spécifiques désignées par l'expression « *Software As A*

[1] Déclaration en date du 11 septembre 2014 du bureau du directeur du Renseignement National et du ministère de la Justice américain, portant sur la déclassification de documents dans le cadre du « *Protect America Act* » (disponible sur le site iconrecord).

Service » (SaaS). Désormais on parle aussi de « *Data As A Service* », ou encore de « *Back-Up As A Service* ». En définitive, les offres « *As A Service* » ont le vent en poupe.

Si ce type d'offres ne constitue pas une nouveauté, qu'elles s'adressent aux professionnels ou aux consommateurs (on en veut pour preuve les boîtes de réception Hotmail, Gmail, etc.), les entreprises ont longtemps stocké données et applications au sein de « *datacenters* » dédiés, de préférence localisés à proximité de leur siège social, sur lesquels elles demeuraient en mesure d'exercer pleinement leur contrôle. La réservation d'un espace dédié au profit d'une entreprise présente cependant un inconvénient majeur, celui de l'absence de souplesse dans la gestion des ressources disponibles, lesquelles peuvent s'avérer bien supérieures aux besoins réels – et bien plus coûteuses que nécessaire - par exemple lorsque les capacités dédiées sont estimées sur le fondement d'un pic d'activité annuel de l'entreprise, alors qu'elles ne peuvent être utilisées de manière optimale tout au long de l'année.

Néanmoins le Cloud Computing rend possible une mutualisation des ressources entre les utilisateurs, ce qui permet de réduire, en les partageant, les coûts de maintenance, d'exploitation, de matériel et d'énergie. Les utilisateurs sont généralement séduits par la possibilité qui leur est offerte d'augmenter ou de réduire très rapidement les ressources disponibles (allocation dynamique) et d'être facturés en fonction de l'usage réel des ressources (« *pay as you go* »).

Que l'on soit d'ores et déjà utilisateur du Cloud computing ou encore dubitatif quant à son utilisation, mieux vaut en tout état de cause connaître les enjeux et les risques du Cloud, et corrélativement les précautions à prendre lors de la conclusion d'un contrat avec un prestataire Cloud.

I. AVANT DE RECOURIR À UN SERVICE CLOUD, IL CONVIENT *A MINIMA* DE S'ASSURER QUE LE CONTRAT PROPOSÉ NE PRIVE PAS LE CLIENT DE LA POSSIBILITÉ DE SE CONFORMER À SES PROPRES OBLIGATIONS LÉGALES

L'externalisation de services informatiques en mode Cloud implique de déléguer certaines fonctions jusque-là remplies en interne. L'externalisation pourra notamment concerner les fonctions d'hébergement, de sécurité, d'entretien et de maintenance de certains éléments du système informatique de l'entreprise. Or, la maîtrise de ces fonctions constitue un enjeu important dans la mesure où ces dernières doivent répondre à un certain nombre d'obligations légales, dont le non-respect est susceptible d'engager la responsabilité de l'entreprise. Externaliser conduit à déplacer la charge de l'exécution de ces fonctions et les moyens de leur mise en œuvre sur le prestataire, sans que l'entreprise cliente puisse pour autant s'exonérer de sa responsabilité en cas de mauvaise exécution de ses obligations par le prestataire.

S'agissant plus particulièrement du traitement de données personnelles, l'entreprise demeure en principe responsable de traitement au sens de l'article 3 de la loi n° 78-17 du 6 janvier 1978 dite « Informatique et libertés ». Garante du prestataire, auquel elle délègue tout ou partie du traitement de données à caractère personnel, il lui incombe donc de veiller au respect par celui-ci des contraintes légales. Ce principe a été rappelé récemment par la Commission

nationale de l'informatique et des libertés (CNIL) dans une décision en date du 7 août 2014[2]. Elle y affirme que le responsable de traitement devra notamment s'assurer que les durées de conservation des données (qui pourront être précisées dans une politique d'archivage) sont respectées dans le cadre du service, que les droits des personnes visées par les traitements sont garantis, et que les restrictions en matière de transfert de données hors de l'Espace économique européen sont prises en compte.

Sur ce dernier point, il convient d'être particulièrement vigilant dans la rédaction et la négociation du contrat de services Cloud. Par principe, la localisation exacte des données n'est pas connue, celles-ci pouvant être déplacées à l'insu même du client, en fonction des disponibilités des serveurs. Toutefois, il pourra être prévu contractuellement que le prestataire de Cloud Computing s'engage à restreindre les implantations de ses datacenters au territoire de l'Espace économique européen ou dans des Etats assurant un niveau « adéquat » de protection des données personnelles. A défaut de telles garanties, la loi Informatique et libertés impose de recueillir l'autorisation de la CNIL préalablement à tout transfert, cette autorisation devant être obtenue pour chacun des Etats à destination desquels un transfert est envisagé ou envisageable. Cet impératif semble en contradiction avec le fonctionnement même du Cloud Computing, et difficile à mettre en œuvre auprès d'un prestataire.

Il convient de noter que le prestataire de services Cloud est susceptible, selon une recommandation de la CNIL[3], d'être regardé comme co-responsable du traitement. A ce titre, il pourrait être tenu des mêmes obligations de conformité à la loi Informatique et libertés que son client dès lors :

- qu'il est établi sur le territoire français ou que, bien qu'établi dans un Etat situé en dehors de l'Espace Economique Européen, il utilise des moyens de traitement situés sur le territoire français ;

- qu'il se comporte comme un responsable de traitement, déterminant, de manière autonome, tout ou partie des finalités et/ou des moyens du traitement, sans se contenter d'agir sur instructions du client et sans lui rendre de comptes.

Il est dans l'intérêt des deux parties que le client conserve une maîtrise aussi grande que possible de ses données hébergées en mode Cloud. Le client sera ainsi en mesure de s'assurer que le traitement est conforme aux obligations susmentionnées ; quant au prestataire, laisser au client la maîtrise de ses traitements lui permettra d'échapper à une qualification le mettant au premier plan de possibles sanctions administratives et pénales. La proposition de règlement général relatif à la protection des données, telle qu'adoptée par le Parlement européen le 12 mars 2014[4], prévoit, d'ailleurs, en son article 26, un régime applicable au sous-traitant dont le respect pourrait conduire à exclure toute hypothèse de coresponsabilité.

[2] Délibération de la formation restreinte n° 2014-298 du 7 aout 2014 prononçant un avertissement à l'encontre de la société Orange.
[3] « *Recommandations pour les entreprises qui envisagent de recourir à des services de Cloud Computing* », CNIL, 25 juin 2012.
[4] Résolution législative du Parlement européen du 12 mars 2014 sur la proposition de règlement du Parlement européen et du Conseil 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 (Règlement général sur la protection des données) (COM(2012)0011 – C7-0025/2012 – 2012/0011(COD)).

A cet égard, rappelons que cette même proposition de règlement aborde, en son article 23, les concepts de protection dès la conception (« *by design* ») et de protection par défaut (« *by default* ») en soulignant, notamment, en son considérant 61, que :

> « *Le principe de la protection des données dès la conception requiert que cette protection soit intégrée dans la totalité du cycle de vie d'une technologie, dès la toute première étape de conception jusqu'à son déploiement final, son utilisation et son élimination. Cela devrait également inclure la responsabilité pour les produits et services utilisés par le responsable du traitement ou le sous-traitant.*
>
> *Le principe de la protection des données par défaut requiert que les paramètres de respect de la vie privée dans les services et produits soient par défaut conformes aux principes généraux de la protection des données, tels que la réduction des données au minimum et la limitation de la finalité.* »

Quel qu'il soit, l'outil de Cloud retenu devrait donc être conçu pour offrir à l'entreprise cliente la possibilité d'assurer par défaut le respect des règles applicables en matière de données personnelles. Les prestataires ne pourront à l'avenir se dispenser de mettre en œuvre de tels paramètres.

Outre ces éléments de portée générale, les prestataires de services en Cloud devront, lorsqu'ils proposent plus spécifiquement leurs services à des personnes publiques, des professionnels ou établissements de santé, être titulaires des agréments nécessaires à l'hébergement des données détenues par ces dernières.

Le Code du patrimoine réserve, en effet, la conservation et la gestion des archives publiques – c'est-à-dire de tous documents qui procèdent de l'activité, dans le cadre de leur mission de service public, de l'Etat, des collectivités territoriales, des établissements publics et des autres personnes morales de droit public ou des personnes de droit privé chargées d'une telle mission – aux personnes agréées à cet effet par le Service Interministériel des Archives de France (SIAF). Le Code de la santé publique prévoit, quant à lui, que les données de santé à caractère personnel, recueillies ou produites à l'occasion des activités de prévention, de diagnostic ou de soins, ne peuvent être déposées qu'auprès des personnes agréées à cet effet, dans le cadre d'une procédure orchestrée par l'Agence des Systèmes d'Information Partagés de Santé (ASIP).

La personne publique, le professionnel ou l'établissement de santé ayant recours à un prestataire non agréé viole ses obligations.

Les listes de prestataires agréés sont disponibles sur les sites respectifs du SIAF et de l'ASIP. Toutefois, parmi les prestataires français de services en mode Cloud dit « Souverain », un seul est à l'heure actuelle agréé par l'ASIP, tandis qu'aucun n'a encore obtenu l'agrément du SIAF.

II. UNE ATTENTION PARTICULIÈRE S'IMPOSE EN MATIÈRE DE SÉCURITÉ, DANS LA

MESURE OÙ LE CLOUD APPARAÎT – À TORT OU À RAISON – COMME PARTICULIÈREMENT EXPOSÉ À CET ÉGARD.

La confidentialité et la sécurité des données sont, non seulement, stratégiques pour l'entreprise, mais elles relèvent également fréquemment d'obligations légales. La loi Informatique et libertés prévoit ainsi que le responsable du traitement est « *tenu de prendre toutes précautions utiles, au regard de la nature des données et des risques présentés par le traitement, pour préserver la sécurité des données et, notamment, empêcher qu'elles soient déformées, endommagées, ou que des tiers non autorisés y aient accès* ».

Dans de nombreux secteurs d'activités, tels que ceux de la santé, la banque ou la justice, le secret professionnel impose aux entités concernées de redoubler d'attention à cet égard.

En cas de divulgation ou d'altération de données personnelles, l'entreprise cliente pourra généralement agir à l'encontre du prestataire fautif, dans le cadre et dans les limites du contrat de services Cloud. Cependant, elle sera elle-même exposée s'il s'avère qu'elle n'a pas imposé à son prestataire l'obligation de prendre des mesures adéquates en matière de confidentialité et de sécurité. Les risques d'atteinte aux données ne sont pas négligeables et la presse spécialisée se fait régulièrement l'écho d'attaques visant les données hébergées dans le Cloud ou de failles de sécurité.

Si la mutualisation des ressources présente d'indéniables avantages en matière de réduction des coûts, elle constitue toutefois un facteur de risques important. Le Cloud, qu'il soit communautaire, public ou hybride, se partage entre plusieurs utilisateurs. Faute de séparations matérielles que permettait la réservation exclusive de datacenters, les prestataires de services Cloud mettent en place des séparations virtuelles qui doivent être imperméables et solides.

La non-localisation des données et applications hébergées en mode Cloud constitue un second facteur de risque majeur. L'hébergement est souvent assuré de manière opaque pour l'utilisateur, lequel ignore l'emplacement géographique du « nuage » de serveurs dont les ressources sont mises à sa disposition. Il n'a souvent pas connaissance des divers sous-traitants susceptibles d'être impliqués dans la fourniture de la prestation. L'Autorité de contrôle prudentiel et de résolution a pu souligner, dans un rapport sur les risques associés au Cloud Computing publié en juillet 2013[5], que les entreprises du secteur de la banque et de l'assurance mettent en avant « *la difficulté à auditer un prestataire, voire à obtenir un droit d'audit, en raison de la multiplication des intervenants et de leur localisation géographique* ».

Les réponses techniques apportées au besoin de confidentialité et de sécurité sont généralement la sécurisation des connexions au service, une authentification stricte, l'utilisation d'un réseau privé virtuel ou encore le chiffrement systématique des données. Les entreprises ayant recours aux services en mode Cloud peuvent utilement se reporter, pour les intégrer au contrat, aux documents de référence rédigés en la matière, comme la norme ISO/CEI 27001 relative à la sécurité de l'information, complétée par la norme ISO/CEI 27002 énumérant les bonnes pratiques pour la gestion de la sécurité de l'information, ainsi que la

[5] « *Analyses et synthèses : les risques associés au Cloud Computing* », Publication ACPR et Banque de France, n°16, juillet 2013.

norme ISO/CEI 27018 relative à la protection des données personnelles hébergées en mode Cloud et la norme ISO/CEI 27017 portant sur d'autres éléments de sécurité spécifiques au Cloud.

L'intensité des négociations et des efforts en la matière sera bien entendu d'autant plus importante que les données concernées seront sensibles.

III. L'ENTREPRISE UTILISATRICE DOIT ÉGALEMENT GARDER UN CONTRÔLE OPTIMAL SUR L'USAGE DE SES DONNÉES HÉBERGÉES, À SAVOIR GARANTIR SON PROPRE USAGE, MAIS AUSSI RESTREINDRE CELUI DE TIERS.

Les occasions sont nombreuses, dans le cadre du Cloud Computing, de perdre la main sur les données qui y sont versées. Ces risques figurent en bonne place parmi les principaux identifiés par la CNIL dans sa recommandation précitée. Il s'agit principalement de la perte de gouvernance sur le traitement, de la dépendance technologique vis-à-vis du fournisseur, des réquisitions judiciaires notamment prises par des autorités étrangères, des failles dans la chaîne de sous-traitance et de l'indisponibilité du service.

Certains de ces dangers peuvent être facilement écartés, encore faut-il penser à les identifier.

Pour pallier les risques structurels – tels que bugs, pannes, indisponibilité des services et donc de ses données et applications – l'entreprise pourra convenir avec son prestataire d'objectifs de disponibilité du service, de temps de réponse moyen et maximum, et surtout de continuité de service et de temps de rétablissement en cas d'interruption – ce dernier point s'avérant vital pour garantir à l'entreprise cliente la continuité de sa propre activité.

La dépendance vis-à-vis du prestataire est également un sujet sensible, puisqu'en cas de résiliation ou d'expiration du contrat quelle qu'en soit la raison, l'entreprise souhaitera bien entendu obtenir la restitution de ses données, et éventuellement la migration de ces dernières pour permettre leur exploitation sur des ressources alternatives lui appartenant, ou gérées par un prestataire concurrent. L'Autorité de contrôle prudentiel et de résolution souligne dans le rapport précité que « *le recours à un prestataire de Cloud Computing créé un risque d'atteinte à l'intégrité globale du système d'information en raison de la perte d'expertise technique, voire de dépendance au fournisseur* ». Cette dépendance ne saurait déplaire au prestataire, et il convient de faire preuve de de prudence en lui imposant une obligation de « réversibilité ». Les dispositions contractuelles devront détailler les modalités techniques de la restitution (dans un format interopérable), prévoir, si nécessaire, un transfert de connaissances, imposer des délais pour la conservation des données à des fins de sécurité ou au contraire leur destruction totale sur les infrastructures du prestataire et de ses sous-traitants, et enfin, anticiper le coût afférent à ces opérations.

Ces diverses obligations, ainsi que des points complémentaires tels que la gestion et la notification des incidents, ou encore l'enregistrement des logs de connexion, apparaîtront dans le « *Service Level Agreement* » (SLA) annexé au contrat. Les utilisateurs profanes disposent désormais d'un outil leur permettant d'appréhender ces concepts dans le modèle de

structure de SLA, présenté à la Commission européenne, le 25 juin 2014, par le « *Cloud Select Industry Group* »[6].

Outre ces engagements techniques spécifiques, d'autres moyens peuvent être employés pour s'assurer contractuellement du sérieux des services qui seront rendus dans le cadre du recours à un service Cloud. En particulier, il serait utile d'obtenir une description de l'architecture des intervenants et sous-traitants participant directement ou indirectement à la fourniture des services, d'imposer confidentialité et clause d'audit, non seulement au prestataire, mais encore à ses sous-traitants, et de stipuler expressément la mise en place de sauvegardes régulières, ainsi que la réplication des données sur des sites distincts.

Pour s'assurer que ces obligations ne restent pas lettre morte dans la pratique faute de pression suffisante, l'application de la loi française et la négociation ferme de toute clause de limitation ou d'exonération de responsabilité du prestataire constituera la clé de voûte du contrat.

Enfin, si la structure même des services Cloud telle que mise en place par le prestataire ne lui permet pas de garantir ces aspects, il faudra s'interroger sur l'opportunité de recourir à ce service pour des données sensibles ou des activités « cœur de métier ».

IV. LES ENTREPRISES LES PLUS MÉFIANTES POURRONT AVOIR RECOURS AU CLOUD DIT « SOUVERAIN » SI LA MENACE DU « PATRIOT ACT » LEUR PARAÎT TROP ALARMANTE.

Les opérateurs, publics ou privés, « *exploitant des établissements ou utilisant des installations et ouvrages, dont l'indisponibilité risquerait de diminuer d'une façon importante le potentiel de guerre ou économique, la sécurité ou la capacité de survie de la nation* », aussi appelés Opérateurs d'Importance Vitale (OIV), sont, par exemple, tenus par le Code de la défense de protéger plus particulièrement leurs systèmes d'information. D'autres entreprises se sentent également concernées par cette préoccupation.

Les textes permettant aux autorités d'Etats tiers d'obtenir communication, auprès du prestataire, des données stockées dans le Cloud par ses utilisateurs – sans le consentement du propriétaire des données et sans l'en informer au préalable – peuvent alors inquiéter. La bête noire des entreprises est le « *Patriot Act* », ou plutôt les textes qu'il amende : la section 1881a du titre 50 du Code des Etats Unis relative aux recherches d'informations dans l'intérêt de la sécurité nationale visant des non-citoyens américains, dit aussi « *Foreign Intelligence Surveillance Act Amendement* » (FISAA) d'une part, et la section 2701 du titre 18 du même Code relative aux demandes de communication portant sur les données des clients des opérateurs de communications électroniques, dit aussi « *Electronic Communications Privacy Act* » (ECPA).

Les auteurs et les juridictions américaines semblent s'accorder sur l'application extraterritoriale de ces textes. Dès lors, les obligations qu'ils prévoient seraient susceptibles de toucher non seulement les prestataires américains, mais aussi toute filiale d'une société américaine ou société ayant des intérêts ou activités économiques sur le territoire américain.

[6] « *Cloud Service Level Agreement Standardisation Guidelines* » (disponible sur le site ec.europa.eu).

Face à cette problématique, la France a soutenu des projets de services de Cloud appelés « souverains », c'est-à-dire hébergés intégralement sur le territoire national, dans le cadre du projet Andromède. Des solutions qui pourront alors être opportunément comparées à celles fournies par d'autres prestataires.

ALLAN ROSAS & ÉLISE GOEBEL

Le contrôle par la CJUE des actes de l'Union relatifs au traitement des données au regard de la Charte des Droits

L'arrêt Digital Rights Ireland et Seitlinger e. a. du 8 avril 2014

ALLAN ROSAS, juge à la Cour de justice de l'Union européenne

ÉLISE GOEBEL, étudiante à l'École de droit de Sciences Po, master Droit économique, mention GBLG

RÉSUMÉ

Depuis l'arrêt Stauder *de 1969, la Cour de justice de l'Union Européenne n'a cessé d'affirmer l'importance de la protection des droits fondamentaux au sein de l'ordre juridique de l'Union. Le Traité de Lisbonne a renforcé la force juridique de ces droits en incorporant la Charte des droits fondamentaux au sein du Traité sur l'Union Européenne, consacrant ainsi leur nature contraignante et intégrée au droit primaire. Dans l'arrêt* Digital Rights Ireland et Seitlinger e.a. *rendu au printemps 2014, la Cour de justice a invalidé la directive 2006/24 prévoyant la rétention des données personnelles par les opérateurs de communications électroniques dans le cadre de la lutte contre le terrorisme au regard de la Charte. En jugeant la directive non conforme aux droits au respect de la vie privée et à la protection des données personnelles garantis aux articles 7 et 8 de la Charte, la Cour a réaffirmé le contrôle qu'elle exerce sur les actes de l'Union, ainsi que la vigueur de la Charte des droits fondamentaux. Cet article revient sur le contexte judiciaire ayant précédé l'arrêt afin d'appréhender l'arbitrage délicat réalisé par la Cour entre la protection des droits et les objectifs d'intérêt public poursuivis par la directive.*

INTRODUCTION

Érigés au rang de droit primaire par leur incorporation au sein du Traité sur l'Union européenne, les droits et libertés fondamentales constituent aujourd'hui l'un des fondements de la constitutionnalisation du droit de l'Union. La Cour de justice des Communautés européennes avait affirmé pour la première fois, en 1969, dans l'arrêt *Stauder*[1], l'existence de droits fondamentaux compris dans les principes généraux du droit communautaire, et n'a cessé depuis d'étendre la protection qui leur est conférée. Ce positionnement de la Cour, à l'égard des droits, a été confirmé par leur formalisation écrite au sein des traités. L'incorporation de la Charte des droits fondamentaux, et la perspective de l'adhésion à la Convention européenne des droits de l'Homme dans l'article 6 du Traité sur l'Union européenne[2], a conféré une nouvelle force juridique à ces droits, renforçant la Cour dans son rôle de garante de l'ordre juridique de l'Union. Après l'entrée en vigueur, le 1er décembre 2009, du Traité de Lisbonne, modifiant le Traité sur l'Union européenne, la Cour a rendu plus de 200 arrêts ou ordonnances citant la Charte. Concernant le respect de la vie privée et la protection des données personnelles, la série d'arrêts rendus par la grande chambre, au printemps dernier, illustre la transformation du contentieux relatif à ces droits. Le 8 avril 2014, la Cour de justice se prononce simultanément dans les affaires *Digital Rights Ireland et Seitlinger e.a.*[3] (C-293/12 et C-594/12) et *Commission contre Hongrie*[4] (C-288/12). Dans la première, elle invalide l'intégralité de la directive 2006/24/CE[5] du 15 mars 2006, qui organisait la rétention des données de trafic par les fournisseurs de services de communications électroniques au sein des États membres. Dans la seconde, elle condamne la Hongrie en manquement pour avoir compromis l'indépendance de son Commissaire à la protection des données en mettant fin à son mandat de manière anticipée. Dans l'arrêt *Google Spain et Google*[6], rendu le mois suivant, la Cour interprète la directive 95/46 sur la protection des données personnelles comme incluant dans son champ d'application le traitement automatisé des données effectué par les opérateurs de moteurs de recherche. La Cour déclare les opérateurs responsables des données rendues accessibles au public par leurs services, et consacre l'existence d'un droit à l'effacement des données sur Internet[7]. En se référant toutes aux protections accordées par les articles 7 et 8 de la Charte, ces trois décisions consacrent les droits au respect de la vie privée et à la protection des données personnelles, et ce dans un contexte de mobilisation européenne sur ces sujets[8]. Toutefois, alors que la Cour se concentre

[1] CJUE, arrêt *Stauder*, 29/69, point 7, 12 novembre 1969.
[2] T.U.E., art. 6, par. 1 : « *Union reconnait les droits, les libertés et les principes énoncés dans la Charte des droits fondamentaux de l'Union européenne* […] *laquelle a la même valeur juridique que les traités.* ». Voir A. ROSAS et H. KAILA, « *L'application de la Charte des droits fondamentaux de l'Union européenne par la Cour de justice : un premier bilan* », Il Diritto Dell'Unione Europea, Anno XVI Fasc. 1, 2011.
[3] CJUE, arrêt *Digital Rights Ireland et Seitlinger e.a.,* C-293/12 et C-594/12, 8 avril 2014.
[4] CJUE, arrêt *Commission/Hongrie*, C-288/12, 8 avril 2014. Voir : K. Lane SCHEPPELE, « *Making Infringement Procedure More Effecive: A Comment on Commission v. Hungary, Case C-288/12 (8 April 2014) (Grand Chamber)* », Eutopia Law, 29 avril 2014.
[5] Directive 2006/24/CE du Parlement européen et du Conseil, du 15 mars 2006, sur la conservation de données générées ou traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public ou de réseaux publics de communications, et modifiant la directive 2002/58/CE (JO L 105, p. 54).
[6] CJUE, arrêt *Google Spain et Google*, C-131/12, 13 mai 2014.
[7] *Ibidem*, points 97 et 98.
[8] L'impact médiatique des révélations d'Edward Snowden au début de l'été 2013 a attiré l'attention sur l'efficacité des protections des données personnelles dans l'Union. Voir par exemple la plainte contre X de la FIDH et de la LDH du 11 juillet 2013, http://www.fidh.org/fr/europe/france/la-fidh-et-la-ldh-deposent-plainte-pour-atteinte-aux-donnees-personnelles-13646/.

sur l'interprétation de la directive 95/46 dans les arrêts *Commission contre Hongrie* et *Google Spain et Google*, elle se prononce directement sur la validité d'une directive au regard des droits fondamentaux dans l'arrêt *Digital Rights Ireland & Seitlinger e.a.* Ce dernier arrêt mérite une attention particulière.

Les deux litiges au principal qui ont conduit à l'arrêt *Digital Rights Ireland & Seitlinger e.a.* interrogeaient la constitutionnalité des transpositions en droit national de la directive 2006/24/CE du 15 mars 2006, sur la conservation de données générées ou traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public ou de réseaux publics de communications. Adoptée en réaction aux attentats de Madrid, puis de Londres, en mars 2004 et en juillet 2005, la directive 2006/24/CE[9] s'inscrivait dans un objectif de lutte contre le terrorisme. Elle faisait peser sur les fournisseurs de services de communications électroniques accessibles au public et sur les réseaux publics de communications une obligation de rétention des données de trafic, de localisation et des données connexes nécessaires à l'identification de leurs utilisateurs ou abonnés[10], pour une période de six mois à deux ans[11]. L'article 5 de la directive énonçait les différents types de données concernées par cette obligation, comprenant aussi bien les moyens de téléphonie fixe et mobile, que les courriers électroniques et la téléphonie sur internet[12]. Seul le contenu des communications était exclu du champ d'application de la directive. Le recours introduit par l'association Digital Rights Ireland, et l'action collective formée par la Kärtner Landesregierung et MM. Seitlinger, Tschohl et 11 128 autres requérants, portaient sur la légalité de l'obligation de rétention des données au regard du droit à la protection des données personnelles. La High Court irlandaise (affaire C-293/12, *Digital Rights Ireland*) et le Verfassungsgerichthof autrichien (affaire C-594/12, *Seitlinger* e.a.) ont sursis à statuer afin d'interroger la Cour de justice de l'Union sur la validité de la directive. Les questions préjudicielles soulevées demandaient en substance à la Cour de juger de la légalité de la directive 2006/24 au regard des articles 7 et 8 de la Charte des droits fondamentaux, garantissant respectivement le droit au respect de la vie privée et le droit à la protection des données personnelles. Le 8 avril 2014, la Cour de justice a déclaré l'invalidité totale et immédiate de la directive.

Difficilement intelligible hors de son contexte, la compréhension de l'arrêt *Digital Rights Ireland* nécessite un retour sur les critiques dont la directive 2006/24 faisait l'objet ainsi que sur les différentes actions ayant précédé la saisine de la Cour (**I**). C'est dans leur continuité que la Cour a pu déclarer l'invalidité de la directive, réalisant un arbitrage entre la protection des droits des personnes physiques et les objectifs d'intérêt public poursuivis par la directive (**II**).

[9] Directive 2006/24/CE, cons. 11. Voir également : Conseil européen, *Declaration on Combatting Terrorism*, 25 mars 2004, http://www.consilium.europa.eu/uedocs/cmsUpload/DECL-25.3.pdf.
[10] *Ibid.*, art. 1.
[11] *Ibid.*, art. 6.
[12] Les données de trafic comprenaient notamment les informations permettant d'identifier la personne physique (nom, numéro ou identifiant et adresse physique de l'abonné ou appelant), les informations permettant d'identifier le type de communication et d'appareil utilisés (numéros de téléphone ou adresses entrants et sortants, heure et durée des appels ou échanges, numéros IMSI, IMEI et IP) ainsi que les informations permettant la géolocalisation de ces appareils.

I. LES ÉVÉNEMENTS AYANT ENTOURÉ LA SAISINE DE LA COUR ET LE CONTEXTE DE L'ARRÊT

Certains ont pu voir dans les différents épisodes entourant l'adoption de la directive 2006/24, et dans sa difficile mise en œuvre dans les États membres, une préfiguration de la solution de la Cour[13]. Que cela soit avéré ou non, il est certain que l'invalidité déclarée de la directive dans l'arrêt *Digital Rights Ireland* provient d'un contexte particulier. La conformité de l'acte législatif européen aux droits fondamentaux était questionnée dès son adoption et s'est reflétée dans les difficultés des États membres pour transposer la directive de manière conciliable avec les constitutions nationales.

A. La dérogation aux droits organisée par la directive 2006/24

La protection de la vie privée au regard du traitement des données personnelles n'est pas une question récente au sein de l'Union européenne. Bien qu'incomplet, un éventail d'instruments visant à garantir cette protection existe et reste aujourd'hui en vigueur. Le principal acte législatif s'y rattachant est la directive 95/46[14] du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel. La directive, toujours en vigueur, vise à protéger les libertés et droits fondamentaux des personnes physiques à l'égard du traitement des données à caractère personnel, tout en garantissant la libre circulation de ces données au sein de l'Union[15]. Elle est complétée par la directive 2002/58[16] du 12 juillet 2002, qui prévoit des règles spécifiques relatives au traitement des données pour le secteur des services de communications électroniques. Les deux instruments mettent en place un certain nombre de garanties censées assurer la protection des données personnelles au sein de l'Union, aussi bien en ce qui concerne la qualité[17] et la légitimation de leur traitement[18], que leur caractère confidentiel[19]. En particulier, l'article 6 de la directive 2002/58 prévoit l'effacement ou l'anonymisation des données de trafic par les services de communications électroniques, dès lors que ces dernières ne sont plus nécessaires à la transmission d'une communication ou pour des raisons de facturation.

Toutefois, au sein des deux directives se trouvent des dispositions permettant de déroger aux garanties qu'elles établissent. L'article 13 de la directive 95/46 et l'article 15 de la directive 2002/58 prévoient ainsi que les États membres peuvent déroger aux droits et obligations prescrites *« lorsqu'une telle limitation constitue une mesure nécessaire, appropriée et proportionnée, au sein d'une société démocratique, pour sauvegarder la sécurité nationale — c'est-à-dire la sûreté de l'Etat — la défense et la sécurité publique, ou assurer la prévention, la*

[13] A. CASSART et J.-F. HENROTTE, « *L'invalidation de la directive 2006/24 sur la conservation des données de communication électronique ou la chronique d'une mort annoncée* », Revue de jurisprudence de Liège, Mons et Bruxelles, 2014 p.954-960.
[14] 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 (JO L 281, p. 31).
[15] *Ibid.*, art. 1.
[16] Directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002, concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive vie privée et communications électroniques) (JO L 201, p. 37).
[17] Directive 95/46, art. 6.
[18] *Ibid.,* art. 7.
[19] Directive 2002/58, art. 5.

recherche, la détection et la poursuite d'infractions pénales». Cette provision est notamment utilisée dans le cas de législations domestiques prévoyant *« la conservation de données »*. Les États européens ont donc pu, grâce à cette dérogation, adopter des législations nationales permettant la rétention des données personnelles par leurs opérateurs de services de communications électroniques sans tenir compte des garanties précédemment énoncées. La directive 2006/24 avait pour vocation de remédier à l'inégalité et à la disparité des mesures nationales[20], en établissant une obligation commune et harmonisée de rétention des données au niveau européen. Ainsi, la Cour relève, comme l'avait fait M. l'avocat général Cruz Villalón dans ses conclusions du 12 décembre 2013[21], que l'article 11 de la directive 2006/24 prévoit la soustraction de la directive à l'article 15 de la directive 2002/58 précitée. L'objectif de mettre un terme à l'évolution hétérogène des législations préexistantes dans les États membres impliquait de déroger aux obligations de contrôle et de protection des données établies par les deux premières directives.

B. Les actions judiciaires concernant la directive 2006/24 et ayant précédé la saisine de la Cour de justice

Dès son adoption, la directive 2006/24 n'a pas été exempte de critiques[22]. Tenus de transposer la directive avant le 15 septembre 2007[23], la plupart des États ont choisi d'utiliser leur faculté de reporter l'obligation de transposition au 15 mars 2009[24]. N'ayant pas transposé la directive dans le délai imparti ou l'ayant mal transposée, plusieurs États membres ont fait l'objet de recours en manquement suite à des procédures engagées par la Commission européenne. L'Irlande, la Grèce et la Suède ont notamment été concernées[25] et une procédure était pendante contre l'Allemagne au moment de l'arrêt[26]. Ainsi, dans son rapport d'évaluation du 18 avril 2011[27], la Commission européenne relevait l'inégalité des transpositions de la directive et le manque d'efficacité de ses traductions en droits nationaux. Le Contrôleur européen de la protection des données, dans un avis du 31 mai 2011[28], affirmait que la directive avait échoué

[20] Directive 2006/24, cons. 5 : « *Plusieurs États ont légiféré sur la conservation de données par les fournisseurs de services … Lesdites dispositions nationales varient considérablement* ».
[21] Conclusions du 12 décembre 2013 de M. l'avocat général Cruz Villalón dans l'arrêt *Digital Rights Ireland et Seitlinger e.a.*, C-293/12 et C-594/12, 8 avril 2014, points 39 et 40.
[22] Dans son Avis 3/2006 du 25 mars 2006, le Groupe de travail « Article 29 » relève déjà que « *la directive ne prévoit pas de garanties spécifiques suffisantes en matière de traitement des données de communication* » (Groupe Article 29, « Avis 3/2006 sur la directive 2006/24/CE du Parlement européen et du Conseil sur la conservation de données générées ou traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public ou de réseaux publics de communication, et modifiant la directive 2002/58/CE », WP 119, 25 mars 2006).
[23] Directive 2006/24, art. 15.
[24] Uniquement en ce qui concerne la mise en œuvre des obligations de conservation relatives à l'accès à l'internet, au courrier électronique par l'internet et à la téléphonie par l'internet. Pour une liste précise des États, voir les déclarations des États membres annexées à la directive 2006/24.
[25] Voir les arrêts suivants : CJUE, arrêt *Commission/Irlande*, C-202/09, 26 novembre 2009 ; CJUE, arrêt *Commission/Grèce*, C-211/09, 26 novembre 2009 ; CJUE, arrêt *Commission/Suède*, C-185/09, 4 février 2010, et arrêt CJUE *Commission/Suède*, C-270/11, 30 mai 2013.
[26] Ordonnance rendue dans l'affaire *Commission/Allemagne*, C-329/12, EU:C:2014:2034.
[27] Commission Européenne, « *Rapport d'évaluation au Conseil et Parlement européen concernant la directive sur la conservation des données* », 18 avril 2011, COM(2011) 225 final, p.10.
[28] Contrôleur européen de la protection des données, « *Opinion of the European Data Protection Supervisor on the Evaluation report from the Commission to the Council and the European Parliament on the Data Retention Directive (Directive 2006/24/EC)* », 31 mai 2011, EDPS 11/6.

à harmoniser les législations nationales, et que ses dispositions étaient établies en violation des droits au respect de la vie privée et à la protection des données.

La Cour de justice, dans un arrêt du 10 février 2009, *Irlande contre Parlement européen et Conseil*[29], avait déjà eu l'occasion d'examiner la validité de la directive 2006/24. La question préjudicielle qui lui avait été posée ne s'intéressait toutefois qu'à sa base légale, et non à sa conformité au regard des droits fondamentaux. Liée par la question préjudicielle, la Cour avait ainsi précisé que son jugement ne la liait que concernant la base juridique affirmée dans l'arrêt, laissant la porte ouverte à un futur examen de légalité au regard de la Charte[30]. En l'absence de compétence pour juger directement de la validité de la directive, certaines Cours suprêmes nationales n'ont pas hésité à examiner la légalité de sa mise en œuvre en droit national au regard des droits fondamentaux. Un contentieux constitutionnel a ainsi précédé la saisine de la Cour de justice. En décembre 2008, la Cour constitutionnelle bulgare[31] est la première à invalider l'une des dispositions transposant la directive. Elle est suivie, le 8 octobre 2009, par la Cour constitutionnelle roumaine[32] qui déclare l'intégralité de la transposition invalide « *au regard du manque de garanties appropriées et suffisantes* »[33]. En mars 2010, c'est au tour du Bundesverfassungsgericht [34] allemand, suivi par les cours constitutionnelles chypriote et tchèque[35], d'annuler les dispositions respectives de leurs droits nationaux organisant la rétention des données, jugées illégales au regard de leurs constitutions respectives et de l'article 8 de la Convention européenne des droits de l'homme sur le respect de la vie privée. Finalement, la High Court irlandaise et le Verfassungsgerichthof autrichien ont saisi la Cour de justice de la question relative à la validité de la directive. La Cour suprême slovène[36], saisie d'une question analogue, a alors sursis à statuer dans l'attente de l'arrêt de la Cour de justice, illustrant la conclusion d'un dialogue judiciaire intra-européen.

Les critiques à l'encontre la directive 2006/24 et le contexte judiciaire précédant la saisine de la Cour de justice forment le terreau de la solution trouvée par la Cour de justice dans l'arrêt *Digital Rights Ireland*. Il n'en reste pas moins que la Cour, saisie du contentieux, a dû déterminer à son tour la nature et l'étendue des violations contenues dans l'obligation de rétention des données, réalisant ainsi un arbitrage délicat entre les droits fondamentaux et l'intérêt de sécurité publique protégé par la directive.

---

[29] CJUE, arrêt *Irlande/Parlement et Conseil*, C-301/06, 10 février 2009.

[30] *Ibid.*, point 57 : « *Il y a lieu de préciser que le recours formé par l'Irlande porte uniquement sur le choix de la base juridique et non pas sur une éventuelle violation des droits fondamentaux découlant des ingérences dans l'exercice du droit au respect de la vie privée que la directive 2006/24 comporte* ».

[31] Varhoven administrativen sad, arrêt n°13627 du 11 décembre 2008. Voir p. 45 du rapport « *Access to information in Bulgaria* », Sofia, 2008, https://www.ip-rs.si/fileadmin/user_upload/Pdf/porocila/tuji_organi/Annual_Report_for_2008__Acces_to_Information_in_Bulgaria.pdf.

[32] Curtea Constitutionala, décision du 8 octobre 2009, n° 1.258, journal officiel n° 723/27 du 23 octobre 2009.

[33] Traduction libre.

[34] Bundesverfassungsgericht, décision du 2 mars 2010, 1 BvR 256/08, 1 BvR 263/08 et 1 BvR 586/08, journal officiel du 1er avril 2011.

[35] Anotato Diskastirio tis Kypriakis Dimokratias, décision du 1er février 2011, n°183(I)/2007 et Ustavni Soud, arrêt du 22 mars 2011, Pl US 24/10. Voir notamment : P. Molek, « *Unconstitutionality of the Czech Implementation of the Data Retention Directive ; Decision of 22 March 2011* », European Constitutional Law Review, Vol. 8, n°2, juin 2012, pp. 338-353.

[36] Ustavno sodisce, arrêt du 26 septembre 2013, n° U-I-65/13-16.

II. La protection des données face à la lutte contre le terrorisme, l'arbitrage de la Cour entre protection des droits et intérêt de sauvegarde de la sécurité nationale

Dans l'arrêt *Digital Rights Ireland*, la Cour de justice affirme l'invalidité de la directive 2006/24 en ce qu'elle ne présente pas les garanties nécessaires pour contrebalancer les violations des droits qu'elle implique. Malgré l'objectif matériel d'intérêt général qu'elle protège, la directive ne satisfait pas aux exigences du test de proportionnalité de l'article 52 de la Charte des droits fondamentaux. Annulant l'ensemble de la directive, l'arrêt confirme la vigueur des articles 7 et 8 de la Charte et renforce, par la liste de garanties qu'elle cite, les standards de protection des données dans l'Union.

A. L'invalidité déclarée au regard de l'absence de proportionnalité entre la violation des droits et l'objectif d'intérêt général de l'Union

Dans la mesure où elles concernent de manière « *directe et spécifique la vie privée* »[37], les dispositions de la directive devaient respecter les droits garantis par l'article 7 de la Charte des droits fondamentaux et se conformer aux exigences de protection des données personnelles découlant de l'article 8. Au regard de l'obligation générale de conservation des données imposée par la directive, M. l'avocat général Cruz Villalón avait déjà considéré que cette dernière constituait une « *ingérence particulièrement caractérisée dans le droit au respect de la vie privée* »[38]. En effet, s'inspirant de la jurisprudence de la Cour européenne des droits de l'homme, l'avocat général avançait que la mémorisation de données relatives à la vie privée d'un individu représente en soi une « *ingérence dans le droit au respect de sa vie privée garanti par l'article 8, paragraphe 1 de la CEDH* »[39]. Non contestée par les parties lors de l'audience, la Cour a déterminé, sans surprise, que « *l'obligation imposée* [par la directive] *constitue en soi une ingérence dans les droits garantis par l'article 7 de la Charte* »[40]. L'ingérence est aggravée par la possibilité pour les autorités nationales d'accéder à ces données[41] et par l'ampleur de la violation que cet accès implique[42].

Cependant, ces violations doivent être considérées au regard de l'article 52 de la Charte et des objectifs poursuivis par la directive[43]. La législation européenne ne portant pas atteinte au « *contenu essentiel desdits droits et libertés* », la Cour a réalisé l'examen de la validité de la directive au regard du « *principe de proportionnalité* » selon lequel les « *limitations ne peuvent être apportées que si elles sont nécessaires et répondent effectivement à des objectifs d'intérêt général reconnus par l'Union ou au besoin de protection des droits et libertés d'autrui* » (article 52, paragraphe 1). S'inscrivant dans la lignée du précédent qu'elle avait établi dans l'arrêt *Volker und Markus Schecke*[44] du 9 novembre 2010, la Cour a procédé à un test de proportionnalité en trois étapes. Après avoir déterminé l'existence d'un intérêt général de l'Union, la Cour examine l'utilité des dispositions de la directive avant de rechercher si ces

[37] CJUE, arrêt *Digital Rights Ireland*, point 29.
[38] Conclusions de M. l'avocat général Cruz Villalón, point 68 et suivants.
[39] *Ibid.*, point 69, citant la CourEDH, arrêt *Leander c. Suède* du 26 mars 1987, série A n°116.
[40] CJUE, arrêt *Digital Rights Ireland*, point 47.
[41] *Ibid.*, point 35 et citant l'arrêt *Leander c. Suède* du 26 mars 1987.
[42] *Ibid.*, point 37.
[43] *Ibid.*, point 38 et s. et conclusions de M. l'avocat général Cruz Villalón, points 133 et s.
[44] CJUE, arrêt *Volker und Markus Schecke et Eifert*, C-92/09 et C-93/09, EU:C:2010:662, 9 novembre 2010, points 65 à 89.

dernières sont strictement nécessaires compte tenu des violations des droits fondamentaux qui en résultent :

- Adoptée pour harmoniser, au niveau européen, la conservation des données par les fournisseurs de services de communications électroniques « *en vue de garantir la disponibilité de ces données à des fins de recherche, de détection et de poursuite d'infractions graves* »[45], l'objectif matériel de la directive était de « *garantir la sécurité publique* », s'inscrivant ainsi dans le cadre d'un « *objectif d'intérêt général de l'Union* » [46] et du « *droit à la sûreté* » reconnu à l'article 6 de la Charte ;

- Concernant l'utilité de la rétention des données, la Cour relève simplement la possibilité pour les autorités nationales de disposer de possibilités supplémentaires afin d'élucider les infractions graves[47] ;

- La directive ne convainc cependant pas la Cour de justice de la stricte nécessité de ses dispositions, caractère qui lui aurait permis de déroger à l'importance particulière de l'obligation explicite de protection des données prévue à l'article 8, paragraphe 1 de la Charte[48]. La Cour constate l'absence de règles claires et précises concernant les garanties régissant la portée et l'application de l'obligation de rétention. En s'inspirant de la jurisprudence de la Cour européenne des droits de l'homme[49], la Cour relève particulièrement les faits suivants :

    - le risque d'accès illicite à ces données renforcé par leur traitement automatique (point 55) ;

    - l'étendue des données concernées par la rétention, et l'aspect généralisé de son application sans « *différenciation, limitation ou exception* » opérées en fonction de l'objectif de lutte contre les infractions graves (points 56 et 57) ;

    - l'absence de relation entre les données conservées et une situation susceptible de donner lieu à des poursuites pénales ainsi que l'absence de distinction entre les données de droit commun et celles relevant du secret professionnel (point 58) ;

    - l'absence de relation entre les données conservées et une menace avérée pour la sécurité publique, permettant la limitation temporelle ou spatiale de la rétention (point 59) ;

[45] Directive 2006/24, considérant 11 et article 1er.
[46] CJUE, arrêt *Digital Rights Ireland*, point 42.
[47] *Ibid.*, point 49 – Certaines réactions immédiates ont regretté l'absence d'enquête plus poussée de la Cour pour estimer l'adéquation de l'outil de rétention des données pour lutter contre le terrorisme (O. Lynskey, « *Joined Cases C-293/12 and 594/12 Digital Rights Ireland and Seitlinger and Others : The Good, the Bad and the Ugly* », 8 avril 2014, European Law Blog). Il existe toutefois une présomption de l'utilité des moyens choisis par les États pour poursuivre les objectifs des législations mises en place. En outre, le rapport d'évaluation de la Commission européenne tend à prouver que la plupart des États membres considéraient les mesures prescrites par la directive comme nécessaires et appropriées et poursuivant des objectifs légitimes (COM (2011) 225 final, p.35).
[48] *Ibid.*, point 53.
[49] *Ibid.*, point 54.

- Enfin, la directive laissait aux États la charge de prévoir les garanties procédurales entourant son application, sans prévoir de critères objectifs délimitant l'accès et l'utilisation des données par les autorités nationales et sans définir la notion « *d'infraction grave* » (points 60 et 61).

L'examen de ces éléments, ajouté à l'aspect arbitraire de la durée de rétention des données[50], a permis à la Cour de déclarer que les dispositions de la directive étaient insuffisantes pour garantir le caractère limité et nécessaire de l'ingérence dans les droits fondamentaux[51]. La Cour de justice achève son raisonnement en ajoutant que la rédaction de la directive présentait également un risque d'abus important relatif à l'accès aux données et à leur utilisation illicite. En effet, l'article 7 de la directive faisait peser l'obligation de rétention directement sur les entreprises privées que sont les fournisseurs de moyens de communications en leur permettant de tenir compte de « *considérations économiques lors de la détermination du niveau de sécurité* » appliqué[52]. La directive ne prévoyait donc, ni la destruction de ces données à l'issue de la période de rétention, ni l'imposition d'une conservation sur le territoire européen sans laquelle il devient possible de soustraire les données en question aux garanties du droit de l'Union[53].

Au regard de ces lacunes, la Cour a jugé que « *le législateur de l'Union a excédé les limites qu'impose le respect du principe de proportionnalité au regard des articles 7, 8 et 52 de la Charte* »[54] concluant à l'invalidité de la directive. Par cette action, et l'argumentaire développé dans l'arrêt, la Cour confirme sa capacité à promouvoir les droits fondamentaux, malgré la pondération imposée par le principe de proportionnalité de l'article 52 de la Charte, et ce pour des actes concernant le domaine particulier de la sécurité de l'État.

B. Les implications de l'arrêt, le contrôle juridictionnel de la Cour de justice sur les actes de l'Union au regard des droits fondamentaux

Salué par de nombreuses instances publiques étatiques[55], l'arrêt aura certainement des implications à long terme, bien que celles-ci soient encore difficilement estimables. En invalidant la directive 2006/24, la Cour ne condamne pas le principe de la rétention des données en lui-même. Elle laisse la porte ouverte à une nouvelle législation communautaire prévoyant une nouvelle obligation de rétention. L'invalidité de la directive au niveau européen n'entraine pas non plus nécessairement l'invalidité de ses transpositions au sein des États membres[56]. En revanche, en précisant les garanties indispensables pour que la limitation des droits reste « *strictement nécessaire* », elle donne au législateur européen et aux cours suprêmes nationales des indications utiles pour se prononcer sur la validité ou non d'une nouvelle législation européenne, ou pour statuer sur celle d'une transposition nationale. Ainsi, dans une récente étude annuelle, le Conseil d'État français note que l'arrêt *Digital Rights*

[50] *Ibid.*, point 63.
[51] *Ibid.*, point 65.
[52] *Ibid.*, points 66 et 67.
[53] *Ibid.*, point 68. La Cour cite notamment la nécessité d'un contrôle garanti par une autorité indépendante telle qu'exigé à l'article 8 paragraphe 3 de la Charte.
[54] *Ibid.*, points 69 et s.
[55] K. KOPONEN, S. REINBOTH, P. SAJARI, « *Finland must revise its data protection laws* », Helsinki Times, 26 août 2014.
[56] Les dispositions nationales restent en effet valides sans contrevenir aux directives 95/46 et 2002/58 dans la mesure où elles s'inscrivent dans la dérogation prévue à l'article 15 de la directive 2002/58 (voir I.A.).

Ireland soulève la question de la conformité de la législation française avec la norme européenne dégagée par la Cour de justice[57]. Dès lors, dans la mesure où la législation française produit une obligation de rétention générale des données similaire à celle de la directive censurée, « *il apparait nécessaire aujourd'hui de procéder à un réexamen global du cadre juridique de la surveillance des communications, dans le but de préserver la capacité* [du] *pays à protéger sa sécurité nationale tout en apportant l'ensemble des garanties nécessaires à la protection des droits fondamentaux, et notamment de la sûreté* »[58]. Sans aller jusqu'à demander l'annulation des dispositions nationales, les rédacteurs de ladite note préconisent la révision et le renforcement des garanties les entourant afin de se conformer aux exigences dégagées par la Cour de justice.

En outre, il convient de relever l'importance de l'arrêt au regard du projet de réforme visant à créer un cadre européen de la protection des données personnelles. Le projet, soumis par la Commission européenne[59], vise à améliorer la cohérence des règles de protection des données personnelles dans l'Union en modernisant la directive 95/46. En négociation depuis le début de l'année 2012, les propositions de règlement et de directive ont finalement été votées par le Parlement européen, peu de temps avant la publication de l'arrêt *Digital Rights Ireland*[60]. Avec déjà près de 4000 amendements soumis au Parlement en première lecture, le projet n'a pas encore été adopté en Conseil des ministres. Les conclusions de la Cour sur l'invalidité de la directive 2006/24 et la liste de garanties prescrites à cette occasion auront certainement une influence sur le projet[61].

L'arrêt *Digital Rights* Ireland du 8 avril 2014 confirme le rôle de la Cour, en temps que juge suprême de l'Union, et ce, tout particulièrement dans un domaine touchant aux intérêts souverains : la lutte contre la grande criminalité. En ce sens, la décision rappelle les conclusions auxquelles la Cour était parvenue dans les arrêts Kadi[62], où elle s'était confrontée à la question de l'illégalité d'actes communautaires découlant de décisions du Conseil de sécurité des Nations unies poursuivant un objectif de lutte contre le terrorisme international[63].

---

[57] Conseil d'État, *Étude annuelle 2014 : Le numérique et les droits fondamentaux*, http://www.ladocumentationfrancaise.fr/var/storage/rapports-publics/144000541/0000.pdf.

[58] *Ibid.*, p.19.

[59] Commission européenne, « *proposition de régulation du Parlement européen et du Conseil sur la protection des individus au regard du traitement des données personnelles et de la libre circulation* », COM(2012) 11 final, 25 janvier 2012 et proposition de directive du Parlement européen et du Conseil relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, COM(2012) 10 final, 25 janvier 2012.

[60] Commission européenne, mémo du 12 mars 2014, « *Progress on EU data protection reform now irreversible following European Parliament vote* », MEMO/14/186, http://europa.eu/rapid/press-release_MEMO-14-186_en.htm/.

[61] Communiqué du ministère de la justice luxembourgeois : « *L'arrêt de la CJUE souligne clairement que tous les droits fondamentaux des citoyens de l'Union européenne sont à respecter* », 9 avril 2014, http://www.gouvernement.lu/3641093/08-cjue/.

[62] Arrêt du 3 septembre 2008, Kadi et Al Barakaat International Foundation/Conseil et Commission, C-539/10 P et C-402/05 P et C-415/05 P, EU:C:2008:461 et arrêt du 18 juillet 2013, Commission e.a./Kadi, C-584/10 P, C-593/10 P et C-595/10 P, EU:C:2013:518.

[63] Pour un commentaire plus approfondi, voir : A. ROSAS, « *Counter-Terrorism and the Rule of Law: Issues of Judicial Control* », in S. de FRIAS, A. MARIA et a., « *Counter-Terrorism: International Law and Practice* », Oxford University Press, 2012, pp. 83-100 et G. LENTNER, « *Kadi II before the ECJ - UN Targeted Sanctions and the European Legal Order* », European Law Reporter, 2013, pp. 202-205.

L'entrée en vigueur du Traité de Lisbonne a profondément modifié l'aspect du contentieux des droits fondamentaux devant la Cour de justice[64] en faisant de ceux-ci un « *ingrédient constitutionnel* »[65] essentiel du droit communautaire. Les juges de Luxembourg invalident pour la première fois une législation de l'Union au regard des droits fondamentaux, le 9 novembre 2010, dans l'arrêt *Volker und Markus Schecke et Eifert*[66], en invalidant certaines dispositions du Règlement 1290/2005 et du Règlement 259/2008 au regard des articles 7 et 8 de la Charte. Dans la lignée de cet arrêt, *Digital Rights Ireland* constitue l'un des rares exemples d'une législation de l'Union invalidée au vu de l'absence de conformité à la Charte. La Cour y réaffirme à la fois l'apanage qu'elle détient sur l'examen de la conformité aux Traités des actes législatifs de l'Union et la vigueur des dispositions de la Charte des droits fondamentaux comme partie intégrante et contraignante du droit primaire.

[64] A. ROSAS et L. ARMATI, « *EU Constitutional Law, An Introduction* », Hart publishing, 2nd ed. 2012, p. 172.
[65] *Ibid.*, p. 161.
[66] CJUE, arrêt *Volker und Markus Schecke GbR et Hartmut Eifert contre Land Hessen*, C-92/09 et C-93/09, 9 novembre 2010 et CJUE, arrêt *Association belge des Consommateurs Test-Achats e.a.*, C-36/09, 1er mars 2011.

MAHASTI RAZAVI & CORALIE VAISSIÈRE

Les innovations contractuelles du Big Data

MAHASTI RAZAVI, avocate associée, August & Debouzy

CORALIE VAISSIÈRE, avocate, August & Debouzy

RÉSUMÉ

La mise en place d'un projet Big Data va conduire l'entreprise à confier une partie de la maîtrise des outils de traitement de l'information à son prestataire. Les contrats régissant les relations entre les différents acteurs des projets Big Data devront en particulier traiter des sujets relatifs à la sécurité/confidentialité des données, à l'encadrement de la responsabilité des différents intervenants, à la propriété intellectuelle et enfin à la restitution des données en fin de contrat.

INTRODUCTION

Big Data[1].

Si cette expression est apparue voilà déjà quelques temps dans le langage des nouvelles technologies[2], son utilisation a connu une croissance exponentielle ces dernières années. Les statistiques reflètent ainsi une forte augmentation des recherches associées à ces mots clefs depuis fin 2011, avec notamment un pic d'activité pour cette expression au mois de septembre 2014[3].

[1] Le terme anglophone « Big Data » est repris en français sous le terme « Mégadonnées ».
[2] G. PRESS, « *A very short history of Big Data* », 5 septembre 2013, http://www.forbes.com/sites/gilpress/2013/05/09/a-very-short-history-of-big-data/.
R. E. BRYANT, R. H. KATZ, E. D. LAZOWSKA, « *Big Data Computing: Creating revolutionary breakthroughs in commerce, science and society* », mise à jour le 22 décembre 2008, http://www.cra.org/ccc/files/docs/init/Big_Data.pdf/.
[3] Notamment l'outil Google Trends, cf. https://www.google.fr/trends/explore#q=big%20data&cmpt=q/.

L'année 2014 aura été riche en nouveautés concernant le Big Data. Pas un jour ou presque ne passe sans qu'un article ne soit publié, une conférence organisée, ou une interview dédiée à ce nouveau mode de valorisation des données. De nombreux acteurs privés ou publics voient même dans le Big Data une véritable révolution technologique qui pourrait constituer un levier de croissance important pour la France et permettre la création de nouveaux emplois[4].

Plus qu'un effet de mode, il semble que le Big Data ait vocation à s'intégrer de manière durable dans le paysage des nouvelles technologies. A cet égard, de plus en plus d'entreprises décident de se lancer dans l'aventure. Du côté des prestataires, des start-up spécialisées voient le jour, et les acteurs traditionnels de l'IT ajoutent le Big Data à leurs offres. Du côté des clients, les entreprises tentent d'appréhender les avantages que pourrait leur procurer une analyse Big Data et de définir les projets pour lesquels une telle solution serait pertinente.

Le Big Data reste en effet un concept aux facettes multiples, difficile à saisir. La règle des 3V – volume, variété, vélocité – permet d'appréhender plus en détail cette notion. Le Big Data se caractérise avant tout par le volume et la variété des données à collecter, stocker, et analyser de manière intelligente, et par la vélocité avec laquelle ces tâches sont réalisées. Parler du Big Data, ce n'est cependant pas seulement faire référence aux nouvelles quantités de données devenues disponibles et aux technologies permettant de les exploiter rapidement, mais c'est adopter une nouvelle démarche stratégique visant à créer de la valeur par l'exploitation à grande échelle de ces données.

L'approche Big Data peut, en effet, permettre à des entreprises de créer de la valeur dans différents domaines. Dans l'application marketing du Big Data, l'une des plus médiatisées, l'analyse de données issues d'outils de transaction (cartes de paiement, de fidélité…), d'objets connectés ou du web (réseaux sociaux, données de navigation…) permet d'obtenir un éclairage nouveau sur les pratiques et centres d'intérêt des consommateurs, et, *in fine*, d'améliorer l'efficacité des actions marketing ciblées, des campagnes de fidélisation, de *retargeting* etc.

Le Big Data ne se limite cependant pas au marketing et il peut également permettre aux entreprises d'améliorer de manière plus générale leurs processus opérationnels, par exemple améliorer la sécurité de leur système informatique en récoltant et analysant l'ensemble des informations émanant de leur système d'information pour en dresser une cartographie objective[5].

Véritable outil de modélisation prédictive, le Big Data peut permettre, en analysant de manière combinée des données publiques et des données internes, une amélioration de la gestion des risques. Dans le secteur des assurances par exemple, le Big Data peut permettre d'obtenir une meilleure connaissance du risque de perte de récoltes en analysant des

[4] F. BOURDONCLE, P. HERMELIN, « *Big Data : la France peut gagner, si…* », Le Monde, 2 octobre 2014, http://www.lemonde.fr/idees/article/2014/10/02/big-data-la-france-peut-gagner-si_4499278_3232.html/.
G. SARLAT, S. DI VITTORIO, O. MOUSTACAKIS, « *Le Big Data, un virage technologique à ne pas rater* », 2 octobre 2014, consulté le … http://www.lemonde.fr/idees/article/2014/10/02/le-big-data-un-virage-technologique-a-ne-pas-rater_4499371_3232.html/. Voir également le plan « Big Data – Nouvelle France Industrielle » lancé en 2013 par Arnaud Montebourg.

[5] O. BARTHE, « *Assises de la sécurité : Le big data au secours de la sécurité* », 3 octobre 2014, http://www.lemondeinformatique.fr/actualites/lire-assises-de-la-securite-le-big-data-au-secours-de-la-securite-58827.html/.

mégadonnées météorologiques, des données relatives aux récoltes et celles relatives aux déclarations de sinistres.

Dans la grande majorité des cas, les entreprises mettant en place des projets Big Data font appel à des prestataires spécialisés pour stocker mais, également, analyser ces mégadonnées. Les prestations fournies par ces spécialistes entrent souvent dans la catégorie du *cloud computing* et plus particulièrement des SaaS (« *Software as a Service* ») puisqu'il s'agit (i) d'héberger, « dans le nuage », de grandes quantités de données et (ii) de fournir, en ligne, des applications permettant de les analyser. Les projets Big Data présentent ainsi un caractère protéiforme, puisqu'ils peuvent à la fois concerner les cas dans lesquels le prestataire fournit l'ensemble de la prestation, à savoir le stockage et l'analyse des données, mais également les cas dans lesquels le prestataire ne fait que stocker les données et mettre à la disposition du client, via un contrat de licence, un outil lui permettant d'analyser lui-même les données qu'il aura chargées sur le *cloud*.

Quel que soit le schéma choisi, la mise en place d'un projet Big Data va conduire l'entreprise à confier une partie de la maîtrise des outils de traitement de l'information à son prestataire. Dans ce cadre, il est nécessaire que les relations entre ces différents acteurs soient bien encadrées juridiquement, tout en prenant en compte les spécificités du Big Data.

Les contrats régissant les relations entre les différents acteurs des projets Big Data devront en particulier traiter des sujets relatifs à la sécurité/confidentialité des données, à l'encadrement de la responsabilité des différents intervenants, à la propriété intellectuelle et, enfin, à la restitution des données en fin de contrat.

I. LA SÉCURITÉ ET À LA CONFIDENTIALITÉ DES DONNÉES

Compte tenu du volume de données stockées et traitées, les projets Big Data posent de véritables défis en matière de protection. Il est impératif que les entreprises s'assurent et sécurisent juridiquement la garantie du caractère confidentiel et privé de leurs données par leur partenaire.

Le prestataire étant le dépositaire des données fournies par son client, il doit en assurer la sécurité, la confidentialité, l'intégrité et la disponibilité tout au long du contrat. Cela signifie, notamment, qu'il s'assure que les données ne soient pas déformées, endommagées ou que des tiers non-autorisés y aient accès. Afin d'encadrer contractuellement une telle obligation, un client qui recourt à une offre non standardisée peut spécifier ses exigences de sécurité/confidentialité dans un cahier des charges et demander la mise en place d'un « Plan Assurance Qualité » qui précise les dispositions prises pour répondre aux demandes spécifiques pendant toute la durée du contrat.

Les projets Big Data mettent en œuvre des données variées ne nécessitant pas le même niveau de protection et n'étant pas toujours soumises à des règles juridiques similaires.

La première grande catégorie de données traitées dans ce type de projet, peut tout d'abord, consister en des données personnelles au sens de la loi du 6 janvier 1978 modifiée, dite loi Informatique et Libertés. C'est notamment le cas lorsque les entreprises analysent à grande

échelle des données provenant de leurs clients pour étudier, par exemple, leurs habitudes de réservation en ligne. Dans un tel cas de figure, même si l'entreprise décide d'externaliser son projet Big Data, elle demeure le responsable du traitement au sens de la loi de 1978 dans la mesure où elle a pris la décision de créer les fichiers, elle les exploite, et décide de leur contenu et de leur finalité. Or, au sens de cette loi, le responsable de traitement doit prendre toutes les précautions nécessaires pour assurer la sécurité des données personnelles qu'il traite. En cas de sous-traitance, la loi précise explicitement que le sous-traitant doit présenter des garanties suffisantes pour assurer la sécurité et la confidentialité des données et que le contrat liant le responsable de traitement au sous-traitant doit comporter l'indication précise des obligations lui incombant à ce titre[6]. Au sein d'un projet de Big Data utilisant des données personnelles, il sera donc nécessaire que le contrat répartisse correctement et clairement les rôles et les responsabilités entre le prestataire et son client en matière de respect des obligations légales concernant le traitement des données personnelles.

Cependant, le Big Data peut également avoir recours à d'autres types de données qui, sans être des données personnelles, auront pour autant une importance stratégique pour l'entreprise et devront être protégées à ce titre. Un projet Big Data peut, par exemple, amener une entreprise à analyser des données à caractère sensible telles que des bases de données et historiques de processus provenant de sa propre activité. Le prestataire devra porter une attention toute particulière à la protection de ces données, et ce d'autant plus s'il s'agit de données couvertes par le secret des affaires. Afin d'assurer la confidentialité de telles données, le contrat devra prévoir une clause encadrant strictement les modalités de communication de ces éléments sensibles. Le prestataire pourra, par exemple, s'engager à reconnaître le caractère confidentiel des données stockées, s'interdire de prendre connaissance du contenu des données au-delà de ce qui est nécessaire pour le traitement du projet Big Data, faire respecter ces obligations par l'ensemble de son personnel, et prévenir le client de tout incident ayant mis en cause la confidentialité des données.

Enfin, afin de croiser différents types de mégadonnées entre elles pour en tirer de nouveaux résultats, il est également possible que les entreprises utilisent des données moins stratégiques ne leur appartenant pas, que ce soit des données publiques, des données publiées et en libre accès sur Internet, ou bien encore des données communiquées par des partenaires de l'entreprise (par exemple des données sur les ventes provenant des fournisseurs de l'entreprise concernée). Le fait que ces données puissent être publiques ne signifie pas pour autant que le prestataire ne devra pas en assurer la sécurité, notamment afin d'éviter qu'elles ne soient modifiées ou endommagées et qu'elles faussent ainsi l'analyse Big Data. De plus, même si ces données ne sont pas stratégiques par nature pour l'entreprise, elles peuvent l'être pour la partie qui les fournit, comme, par exemple, pour les fournisseurs qui acceptent de communiquer leurs données sur les ventes, les prix, les produits etc.

Une réflexion devra ainsi être menée par l'entreprise cliente pour déterminer la valeur des données qu'elle confie au prestataire. Cette réflexion aura un impact, non seulement sur le niveau de sécurité et de confidentialité exigé de son partenaire, mais également sur l'éventuel plafond de responsabilité prévu en cas de vol, perte ou destruction des données, ou les assurances couvrant les risques contractuels de part et d'autre.

[6] Article 35 de la Loi Informatique et Libertés, 6 janvier 1978.

Enfin, si une obligation de sécurité et de confidentialité des données pèse sur le prestataire, il revient également au client de maîtriser sa propre politique de sécurisation de ses données. Le prestataire pourra, par exemple, exiger que le client s'engage contractuellement à mettre en place une politique de sécurité interne efficace et qu'il s'assure de certaines sauvegardes des données remises initialement au dit prestataire.

II. LA RESPONSABILITÉ DES DIFFÉRENTS ACTEURS

Le contrat établi entre le client et son prestataire de services Big Data constitue la grille de lecture des parties tout au long de la relation contractuelle, qu'il s'agisse de déterminer les tâches dévolues à chacun ou de régler les questions ayant trait à la responsabilité.

A. Définition du rôle de chacune des parties

Compte tenu de la nouveauté et de la diversité des projets Big Data qui peuvent concerner des données variées et s'appuyer sur des algorithmes d'analyse multiples, il est nécessaire, dans un premier temps, que le contrat définisse avec précision les rôles de chacun des acteurs. Déploiement et exploitation des serveurs, qualification et nettoyage des données, développement puis mise en production des algorithmes… autant de tâches qu'il conviendra d'attribuer précisément à l'une ou l'autre des parties, et pour lesquelles tout juriste requerra l'assistance des équipes techniques concernées par le projet.

Les résultats d'un projet Big Data dépendant fortement de la source initiale d'information, c'est-à-dire les données fournies par le client, et celles-ci pouvant être récoltées et analysées en temps réel, il sera, par exemple, nécessaire de définir quelle partie sera en charge de la certification des données, de la suppression des fautes de frappes, de capteurs, ou encore de la suppression des évènements extrêmes, à même de fausser l'analyse. La définition de la méthodologie d'analyse et le développement de l'algorithme correspondant devront également être assurés en collaboration entre les deux parties, avec une définition précise des rôles de chacun.

B. Définition du niveau de service garanti

Les documents contractuels doivent préciser la nature et l'étendue du service rendu par le prestataire au client. Une telle documentation contractuelle constitue, entre les parties, le référentiel de conformité. Dès lors, la clarté et la précision de leur rédaction sont essentielles. Si chaque projet est porteur de ses spécificités, il sera toutefois important de traiter, dans le contrat de Big Data, des questions de volumes de données, de leur évolutivité quantitative, de la capacité du client à rajouter ou retirer certaines données, de l'accessibilité et de la disponibilité du système. Dans certains cas, les parties pourront convenir d'un *Service Level Agreement* (dit « SLA »). Ce document précise les engagements de performance comme par exemple la possibilité de traitement d'une quantité minimale de données, l'évolution de la quantité de données, les délais de prise en compte de demandes spécifiques, la performance de la sécurité du système etc.

C. Chaînes de responsabilité

Les contrats de prestations portant sur du Big Data peuvent faire intervenir une pluralité d'acteurs, tels que le prestataire assurant l'hébergement des données, celui fournissant les applications d'analyse, celui réalisant l'analyse à proprement dite, etc. Quand bien même il est envisageable qu'un seul et même prestataire assure, vis-à-vis du client final, l'ensemble de la prestation et demeure donc responsable de l'ensemble de ladite prestation, vis-à-vis dudit client, il n'est pas rare que le prestataire recourt lui-même à des cocontractants pour effectuer une partie des tâches qui lui incombent.

Si le prestataire principal demeure contractuellement responsable vis-à-vis du client, celui-ci doit s'assurer qu'il répercute sur tous ses co-contractants, par le biais de contrats miroirs, les engagements qu'il prend vis-à-vis de son client que ce soit, par exemple, en termes de niveaux de service ou de sécurité des données. Ceci lui permettra d'anticiper, dans la mesure du possible, la détermination et la répartition des responsabilités, afin de pouvoir se retourner contre ses cocontractants en cas d'action en responsabilité menée par le client.

D. Limites de responsabilité

En droit français, l'on peut considérer comme un « standard » le principe de la responsabilité d'un prestataire pour les dommages directs causés au client et l'exclusion de la responsabilité pour les dommages indirects.

Dans certains cas, les contrats pré-qualifient plusieurs dommages comme étant des dommages indirects. A cet égard, si la pré-qualification des dommages indirects est acceptée par la jurisprudence, il conviendra de veiller à ce que l'exclusion de responsabilité ne soit pas trop importante au point de contredire la portée de l'obligation essentielle du prestataire, sous peine de risquer de voir la clause concernée réputée non-écrite[7]. En application de ce principe, la jurisprudence a ainsi, récemment, considéré que le fait d'exclure la réparation de tous préjudices financiers, commerciaux, pertes d'exploitation et de chiffres d'affaires et pertes de données, c'est à dire tout préjudice de nature professionnelle, contredisait l'obligation essentielle du contrat qui était, justement, la fourniture d'une ligne adsl pour les besoins d'une activité professionnelle[8].

Si le contrat du projet Big Data comprend une limitation financière de la responsabilité du prestataire, la question de la détermination de ce plafond se posera tout naturellement entre les parties. Le plafond de responsabilité pourra éventuellement correspondre à la valeur du contrat. Toutefois, il conviendra de faire évoluer ce plafond en fonction de la nature, de la sensibilité du projet et des risques découlant, pour le client, d'une défaillance contractuelle du prestataire.

III. LA PROPRIÉTÉ INTELLECTUELLE

De multiples questions de propriété intellectuelle peuvent se poser au sein des projets Big Data suivant leur nature (nature des données, développement des logiciels d'analyse…). Lors de la rédaction du contrat il s'agira impérativement d'aborder deux grandes problématiques :

[7] Cass. Com., 29 juin 2010, n° 09-11841, *Faurecia / Oracle* : « *est réputée non-écrite la clause limitative de réparation qui contredit la portée de l'obligation essentielle souscrite par le débiteur* ».
[8] CA Reims, 4 juin 2013, RG n°11/03323.

- Le droit d'utilisation des logiciels d'analyse : dans l'hypothèse où le prestataire met à la disposition du client un logiciel lui permettant d'analyser lui-même ses mégadonnées, le contrat Big Data devra comprendre les garanties habituelles existant en matière de propriété intellectuelle. Le prestataire devra garantir qu'il détient les droits et autorisations nécessaires à l'utilisation, par le client, des applications d'analyse. La clause propriété intellectuelle définira avec précision les modalités d'utilisation de ces applications par le client, sachant que toute utilisation allant au-delà des droits qui lui sont octroyés pourra constituer une contrefaçon des droits de l'éditeur du logiciel ;

- La propriété des bases de données : dans l'hypothèse où les ensembles de données croisées constituent des bases de données protégées au titre du droit *sui generis* ou au titre du droit d'auteur, le client pourra s'assurer que leur analyse, par le prestataire de service, n'a pas pour effet de lui conférer un droit sur ces bases de données initiales. La clause de propriété intellectuelle pourra donc prévoir que le prestataire n'acquiert, du fait de l'exécution du contrat, aucun droit de propriété sur les données initiales qui lui sont transférées par le client et qu'il traite pour lui.

  Par ailleurs, si le résultat de l'analyse Big Data est lui-même présenté sous la forme d'une base de données protégeable, il reviendra aux parties de décider de la répartition de la propriété de ce résultat et de ne pas laisser dans le vide cette thématique qui ne pourra que donner lieu à des divergences d'interprétation de la part des différents protagonistes. Selon le *business model* des acteurs Big Data, et au regard de la nature de la prestation fournie (enrichissement, classement, ordonnancement des données…), la propriété de la base de données pourra revenir aussi bien au client qu'au prestataire. Le résultat de la négociation menée entre les parties sur ce sujet devra figurer clairement au sein du contrat Big Data.

IV. FIN DU CONTRAT ET RESTITUTION DES DONNÉES

La fin de la relation contractuelle doit permettre au client de décider du sort des mégadonnées stockées et analysées par le prestataire.

Selon le type de données et la finalité de l'analyse Big Data, le client pourra, par exemple, décider que les données soient définitivement supprimées par le prestataire à la fin de la relation (à titre d'exemple, s'il s'agit de données publiques qui ne représentent pas de valeur en tant que telles pour l'entreprise), mais il peut également souhaiter en obtenir la restitution. Dans ce cas, le contrat devra préciser les modalités au titre desquelles le client procèdera, avec l'assistance du prestataire, à une ré-internalisation des données dans ses propres infrastructures lui permettant de poursuivre lui-même l'exploitation de ces données.

Le contrat pourra également prévoir le transfert des données à un autre opérateur, afin de lui confier la poursuite du projet Big Data, ou la mise en place d'un nouveau projet.

La fin de la relation contractuelle se doit donc d'être envisagée dès la rédaction du contrat, en organisant les conditions de mise en œuvre de la réversibilité, ainsi que sa préparation et, le cas échéant, les modalités de calcul de son coût. Le contrat encadrant le projet Big Data devra

notamment clarifier les modalités de transfert des données (format, délai…), les modalités d'assistance du personnel du prestataire à la réalisation de la réversibilité (temps consacré, nombre de personnel…) et les modalités de la collaboration entre les deux parties.

Un manquement à l'obligation de réversibilité des données peut engager la responsabilité du prestataire. Récemment, une entreprise prestataire a, par exemple, été tenue responsable pour ne pas avoir permis la réversibilité des données de son client, et il lui a été fait injonction, soit de fournir sans délai les moyens techniques de nature à permettre au client d'exporter l'ensemble de ses données, soit de lui garantir qu'elle lui assurerait, dans les mêmes conditions tarifaires, la prolongation de l'accès complet au service jusqu'à l'expiration d'un délai de deux mois, à compter du jour où elle sera en mesure de procéder à cette exportation[9].

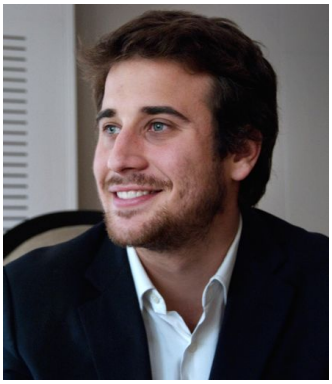
Si les opérations de réversibilité se révèlent trop difficiles à anticiper au stade de la conclusion du contrat, par exemple en raison d'incertitudes concernant le volume de données traité, il est possible que les parties prévoient de renvoyer l'élaboration du plan de réversibilité à un délai ultérieur lors de l'exécution du contrat, et que celui-ci soit mis à jour au fur et à mesure de son exécution.

La rédaction du contrat encadrant les relations entre le client et son prestataire de services Big Data est donc un exercice important mais parfois délicat qui exigera une grande rigueur et une approche très pragmatique impliquant *a minima* techniciens, chefs de projets et juristes, pour assurer une sécurité juridique au bénéfice des deux parties tout au long de la relation contractuelle.

[9] TGI Nanterre, Ordonnance de référé, 30 novembre 2012, *UMP / Oracle*.

JOSEP-MARIA GUERRA

European robots: an umbrella under the rain



JOSEP-MARIA GUERRA

Lawyer, Clifford Chance, Barcelona

jm.guerra@alumni.ie.edu

ABSTRACT

The regulation of robotics is, in fact, an expanding field within the Law and broader Public Policy. The Academia has been interested in this discipline whose *raison d'être* is based on establishing limits on a technology which is called to reshape our society. However, a detailed study of the regulation to be given to open-robotics is often overlooked, even though it has the ability to make the technology accessible to a broader spectrum of the population, narrowing the economic divide and reducing security risks. This paper discusses the fundamentals of this technology and takes as an example the existing Products regulation in the European Union which, after careful reading, can be said to protect open-robotics due to its markedly social character.

INTRODUCTION

Disruption of robotic technology is a fact. The European Union is financing different projects to study ways of regulating emerging scientific and technological developments. Specifically, the RoboLaw project has assessed on the legal implications of this (not so) new technology by delivering "Guidelines on Regulating Robotics". Nevertheless, the creation of a new body of laws is not a pacific assumption as existing laws are, in most cases, applicable to many of the areas that are affected by this technology.

While part of the doctrine considers that a new regulation on product liability is needed to reduce producers liability and incentivize the disruption of this technology, we should also think on the fundamentals of this disruption, whether if it should be open to all or just for a few. Existing European legislation limits the liability of robotics producers depending on the kind of code introduced into the robot. A reading of the Defective Products Directive (DPD) shows how flexibilized liability rules are present in article 7 of the DPD.

I. WHAT IS A ROBOT?

The term "robot"[1] has not found an agreed legal definition[2]. Nevertheless, its features help gain an understanding of how this disruptive technology should be classified[3]. Indeed, there are two main pillars that configure robots: software and hardware[4]. In this sense, both software and hardware have become a unity that creates intelligent machines, artifacts (or artificial organisms) capable of doing a wide variety of tasks[5]. The spectrum of activities that a robot is capable of executing increases due to its learning abilities[6], but also depends on the task set integrated in the robot (hence, software can also act as a constraint for the robot). Therefore, first distinction of robots can be done based on the nature of the performed task or its functionality (e.g. industrial robots, social robots, sexual robots, medical robots...[7]). Notwithstanding robot particularities, all have common features such as the incorporation of effectors, sensors or processors[8] that make them (inter)act as artificial bodies in a human environment. Namely, general[9] robotic features are: (i) autonomy[10], (ii) mechanical

[1] ISO 8373 defines robots as "actuated mechanism programmable in two or more axes with a degree of autonomy, moving within its environment, to perform intended tasks". This definition has been introduced in the "Suggestion for a green paper on legal issues in robotics" (Leroux et al.) in the context of The European Robotics Coordination Action produced by 21 co-authors. In a more recent study, the RoboLaw project has failed to deliver a clear definition of the term 'robot'. *See* Palmerini, E. et al "Guidelines on Regulating Robotics", RoboLaw, SSSA, 2014, p. 15

[2] Some authors have suggested that robots and AI agents should be treated as semi-persons. For instance, in its work, Lehman-Wilzig states that "...AI humanoid may gradually come to be looked on in quasi-human terms as his intellectual powers approach those of human beings in all their variated forms-moral, aesthetic, creative and logical...". *See* Lehman-Wilzig, S.N. "Frankenstein unbound: Towards a legal definition of Artificial Intelligence", p. 447.

[3] Despite there might not be a common legal definition, we should take into account what science considers AI is. In this sense, Kemany beliefs that AI mechanisms could be considered as alive, and therefore called an organism based on six features: metabolism, locomotion, reproducibility, individuality, intelligence and non-artificial composition. *See* Kemany, J.G. "The Man and the Computer", New York Charles Scribner's Sons, 1972, p. 10.

[4] Softbots are excluded as this paper only addresses the impacts of embodied software while bots are intelligent agents that operate virtually.

[5] Besides industrial applications, service robots perform tasks such as domestic (e.g.Roomba) or scientific tasks (e.g. Mars Rovers).

[6] The teaching role of the user is going to force manufacturer and coder to introduce additional constraints into the system, in order to avoid undesired damages. For a clear vision on robot learning capabilities *see* León, A.; Morales, E; Altamirano, L.; Ruiz, K. "Robot New Tasks Through Imitation and Feedback" Lecture Notes in Computer Science Volume 7042, 2011, pp. 549-556.

[7] Euron Robotics Research Roadmap classifies robots as: humanoids, advanced production systems, adaptive robot servants and intelligent homes, network robotics, outdoor robotics (land, sea, air, space), healthcare and life quality robots, military robots and edutainment (what includes robotic art).

[8] Robotic parts have its origin on primitive embodied machines such as the Cooperation Objects. The different sensors and actuators help the machine to perform the tasks to it assigned. For a detailed explanation *See* Ollero, A., Wolisz, A. and Banătre, M. (2010) An Introduction to the Concept of Cooperating Objects and Sensor Networks, in Cooperating Embedded Systems and Wireless Sensor Networks (eds M. Banâtre, P. J. Marrón, A. Ollero and A. Wolisz), ISTE, London, UK.

[9] Robots may also have additional features depending on their particularities.

[10] Ryan Calo, quoting Stephen Johnson, argues that the word autonomy should be substituted by emergenc, a concept firstly introduced by Arkin in 1998. Calo suggests that the word emergence is more adequate to the real decision-making process in robotics, that are not completely autonomous. Nonetheless, autonomy is not an absolute concept so I rather attach to the general concept of autonomy that will be explained in next pages. For

embodiement and (iii) learning ability[11]. As it can be inferred from this first classification, each functionality has its own impact on human life schemes. For instance, social robots[12] bring new challenges to society (as well as to academia) by adding an emotional element to human-machine interaction. The disruption of *social robots* or humanoids is especially important to us as they are a compendium of most physical and computational components of general robots[13]. The term social robots[14] is used to refer to robots with human shape that would be more likely to interact with humans than those keeping its mechanical appearance due to its structure and complexity[15]. This enables social robots to be used in endless environments, such as entertainment or as knowledge vehicles (edutainment)[16]. Human appearance, decision-making and autonomy, therefore, open door to discussion on moral rights assignment still if its complete autonomous development may never arrive[17].

As it will be explained, autonomy is based on the extent of decision capacity of the robot that directly depends on its code, guiding its body and actions. The designed functionality for a given robot is only physically fulfilled through hardware completion: even if robots can also perform tasks that do not have any impact on the physical environment, embodiment remains its main feature. Thus, both software and hardware are necessary conditions for the activity and autonomy of the robot that is to be created for intent. This is, functionality inserted by the developer both in close and open source[18] software, which can be considered as the base technology. As to computers, robot brain[19] can be integrated into the software as package

---

further reading *see* Calo, R. "Robotics and the New Cyberlaw" (February 28, 2014). California Law Review, Vol. 103, 2015. Available at SSRN: http://ssrn.com/abstract=2402972 p. 126.

[11] Calo suggests other features such as social meaning and the aforementioned emergence. The latter has already been discussed. Nevertheless, even if social robots are likely to generate a major impact of robotics and robotics mainstream, other types of robots should not be forgotten. For that reason, Social Meaning must be a feature reserved to Social Robots and other analogous functionality automats. *Op. Cit*. p. 131.

[12] For a specific definition, *see*, e.g., Darling, K. For +: Hegel, F., Muhl, C., Wrede, B., Hielscher-Fastabend, M., Sagerer, G. (2009) "Understanding Social Robots", in: The Second International Conferences on Advances in Computer-Human Interactions (ACHI). Cancun, Mexico: IEEE, p. 169 - 174 ("...physically embodied, autonomous agent that communicates and interacts with humans on an emotional level...").

[13] For a deeper analysis *see* Duffy, B. "Fundamental issues in social robotics" or Becker, B. "Emotional agents naturalizing man-machine interaction", International Review of Information Ethics: Ethics in Robotics; Vol. 6 (12/2006).

[14] *See* Breazeal, C., Takanishi, A., and Kobayashi, T.; "Social robots that interact with people", eds. Springer Handbook of Robotics. Berlin, 2008, pp. 1349-1369.

[15] *See* Warwick, K "Implications and consequences of robots with biological brains", Springer Science+Business Media, 2010.

[16] *See* Becker, B. "Social Robots-Emotional Agents: Some Remarks on Naturalizing Man-Machine interaction". International Review of Information Ethics: Ethics in Robotics; Vol. 6 (12/2006) p.38.

[17] Contrary to what part of the industry affirms, some authors suggest that robot human-like autonomy may be reached in a near future. For instance, Ray Kurzwail suggests that human brain can be recreated, so that engineering, due to the capacity that it has to amplify natural phenomenon, will be able to replicate the neocortex algorithm through the Pattern Recognition Theory of Mind. For a more detailed explanation *See* Kurzwail, R. "How to create a mind: The secret of human thought revealed", Penguin Books, 2013.

[18] Diana M. Cooper referred to close-robotics as those being "narrow function robots" due to close software or hardware whilst open-robotics are characterized by its open-source software and hardware. Misuse of software close-robot would imply liability in copyright basis or software law basis whilst hardware hacking may imply a patent infringement. "We Robot 2013" conference: "A Licensing Approach to Regulation of Open Robotics"; Stanford, 8th of April 2013. Conference video available at: http://www.youtube.com/watch?v=hX_1c1XvJII (Last access: 11th of January 2014).

[19] Many researchers have recently focused in the physical embodiement of the robot brain. It can be configured by different structures that replicate human structures. *See*. e.g Kurzwail, R "how to create a mind" where the author argues that brain complexity will be soon replicated. Nonetheless, some physical replications such as the

software -proprietary software- (e.g. Windows 7 or Mac OX) delivered by mainstream manufacturers in order to facilitate the computer interaction to the user; or it can be created as Open Source Software, an open code available to all users.

Open and close robotics

The features of both software sources might be made appropriate for countless motivations but one thing is clear, the origin of its creation is founded in radically different principles. On the one hand, commercial software is sold by licensing the use, jealously guarding the exclusive rights that belong to the publisher[20]. This means that commercial or proprietary software boosts monopolies on Intellectual Property while, on the other hand, other forms of software have been created in order to permit access to information to those willing to use the code. This boosts a shared developing environment[21].

The sustainability of the so-called Open Source Software is the existence of feeders and companies willing to share its works under certain conditions and specific licenses[22]. For that reason no fees or royalties are charged to the user. It is to say that, due to the beneficial implications, this environment is not only populated by non-business users, but also by a complex spectrum of companies and groups committed to a system that benefits businesses[23] and society as a whole. It also happens in the field of robotics, in which all industry spearheads converge.

Benefits of this technology are endless. Some of them are (i) the lack of control by a unique party on the way the software and in our case, the robot, is used, so (ii) industry technical development is delegated to a dispersed group of creators and monopolies are less likely to emerge. Moreover, (iii) all users create rules and (iv) no "black boxes"[24] can exist: licenses tend to oblige users to show the code and the functioning of the software. Furthermore, (v) transmission of modified versions of the source code cannot be economically charged due to

---

MultiElectrode Array cannot be considered as perfect replications as consciousness rests as an unreachable field, *see* Warwick, K. "Implications and consequences of robots with biological brains" Springer Science+Business Media B.V. 2010.

[20] *See* Forge, S. "The rain forest and the rock garden: the economic impacts of open source software", 2006, Vol 8 No. 3 pp. 12-31, Emerald Group Publishing Limited.

[21] *See* infra Part IV.2. "Boosting shared development".

[22] Some licenses include distribution restrictions. Nevertheless, authors, coders and developers have a wide range of licenses to use so that the chosen license better fits into their needs. The BSD license has been developed by the Open Source Initiative. Information concerning the BSD. Simplified License is available at: http://opensource.org/licenses/BSD-3-Clause. To be considered as Open Source License or GPL-Compatible free software licenses it has to beapproved by the Open Source Initiative and the Free Software Foundation, respectively. *See* "Various Licenses and Comments about Them" GNU Operating System, Available at http://www.gnu.org/licenses/license-list.en.html.

[23] Open Source Software and Robotic companies increase every day. Some examples are: WillowGarage, Arduino, RedHat or CentOs.

[24] A black box is a scientific concept referring to systems that do not allow knowing the internal process but only know its inputs and outputs. For a plane explanation see Wikipedia: http://en.wikipedia.org/wiki/Black_box .

the lack of marketing pressures. Finally, (vi) the delivered product is usually of high quality[25] and commercial success of open-source platforms show high reliability of these systems[26].

In other words, one of the main reasons by which open-software is adequate for risk management is the capacity to boost security in an open peer-review environment, where users can detect and suggest solutions for existing errors in the system. However, it cannot be ignored that embodied software, having much bigger impact in the environment due to its physical presence, needs even more means to detect errors and to prevent damages before they occur.

Hence, Open Source Software applied to robotics is not only an advantage in economic terms but it can also be a security enhancer[27]. Besides security, open-robotics also presents benefits in terms of social development [28]. Contrary to proprietary robotics, open-robotics manufacturers make the product available to all society through the internet[29] and barriers of entry do not exclude anybody from technological development[30]. This clearly represents the materialization of the fight against technological divide, a risk that the industry and *academia* is willing to erase[31].

In terms of security, information era is based in networked systems that include high amounts of data to be transmitted and processed in uncountable manners by millions of users. Highly complex information structures make that complete security cannot be reached based on foreseeability of result[32]. Hence, it makes more difficult to assign an amount of predictability to information products as there is always risk of error: the result is not always the expected.

---

[25] For further detail *see* González-Barahona, J.M; Daffara, C. "Free Software/Open Source: Information Society Opportunities for Europe?", Working Grouo on Libre Software, April 2000. Available at http://eu.conecta.it/paper/ (Last access: june 18th, 2014, 11:14 am).

[26] One of the most recent examples of open-source business model is the CentOS-Red Hat joint venture. When firstly CentOS used Red Had source system and improved it, Red Hat's reaction was to require to erase its name from commercial advertising to protect its own trademark. Nevertheless, shown the improvements on the code introduced by CentOS the corporation has recently opted for joining forces in the market. For a wider picture read "Red Hat and the CentOS Project Join Forces to Speed Open Source Innovation" The Wall Street Journal, January 7, 2014 Available at: http://online.wsj.com/article/PR-CO-20140107-911096.html (Last access: 8th of January 2014). Other well-known examples are Linux or Apache; the latter is used by IBM as a commercial base software that is modified and improved by different users. Hence, we see that the same players that support the IPR current system are also benefiting from new ways of "remix" creation.

[27] *See* Calo, R. "Open Robotics", Maryland Law Review, Vol. 70, No. 3, 2011, the author describes the existing discussion in terms of security in robotics. Other authors argue that OSS is an opportunity to share the existing problems and create shared solutions, contrary to proprietary software. See also Forge, S. Op. Cit. P. 25: " [whilst] OSS exposes flows and cures them [...] proprietary black box model of closed source neither admits security gaps nor allows them to be explicitly tested".

[28] Open-robotics allow the creation of a robot with low budgets, as the greater part of the robot has already been developed and can be acquired without payment of any fee or royalty.

[29] *See* supra note 100. iCub (as all OR or OSR) make available all information concerning the robot to allow users to build its own robot by themselves.

[30] The fact that all stakeholders have access to perfect information could mean the multiplication of opportunities in industry and elimination of monopolies.

[31] For an interesting essay on the concept and the new risks society is facing *see*, e.g., Jackson, L. et al. "Race, Gender, and Information Technology Use: The New Digital Divide", CyberPsychology & Behavior, Volume 11, Number 4, 2008.

[32] Despite information loopholes, there are ways to enhance security through checklists, exhaustive analysis, Mechanistic Engineering Security Development Methods, for further explanation *see* Baskerville, R.

Consequently, when referring to robot foreseeability no exceptions can be done. It would be more accurate to link security expectations to the output that the system has to achieve (i.e. the decisions to be taken in a certain context) rather than to the specific code to be introduced into the robot (in brief, to constrain legally the software characteristics would imply a shrink for computing and scientific development). It is easier for the lawgiver to describe the results to be forbidden to the robot (i.e. harm described by the algorithm dont-disturb[33]), than to rule all the ways how information should be processed. Therefore, since the probability of error exists in all types of information systems, the need to find a base technology that best guarantees an acceptable degree of risk[34] becomes glaring in robotics. Accordingly, the legal status of the aforementioned base technologies should be clarified (especially as it relates to liability). In this sense, the most successful regulation seems to remain product laws[35].

II. THE ILLUSION OF MORAL RIGHTS

Measurability of the degree of autonomy depends on the decision process of the robot[36], which is the essence of cognitive features in autonomous entities. Present robots are created with learning abilities, and its extent determines the degree of autonomy granted to a specific robot. In this sense, autonomous robots should be understood as those making the most important decisions of the tasks assigned to it[37]. Nevertheless, an entity deciding between two options is not to be considered as a moral right-holder in analogy to human beings or even, animals[38] [39]. Morality depends more on the emotions and consciousness rather than the ability to decide[40]. Although decisions may be conditioned by moral reasoning[41], they are not

"Information Systems Security Design Methods: Implications for Information Systems Development", School of Management, Binghamton University, New York, 1993.

[33] Daniel Weld and Oren Etzioni argue that as long as robotics actually concerns primarily with "kinematics, dynamics, path planning, and low level control issues" we could refer to agenthood. *See* Weld D.; Etzioni, O. "The firs Law of Robotics (a call to arms)", Department of Computer Science and Engineering, University of Washington.

[34] At this respect, RoboLaw makes a very fine exposure of the need to achieve an agreement on the acceptable degree of risk that consumers and society should assume. Palmerini, E. et al. "Guidelines on Regulating Robotics", RoboLaw, SSSA, 2014, p. 55 -68.

[35] *See* infra Part IV.

[36] Scholars have distinguished between strong and weak autonomy. Depending on the extent of the decision making capacity of the robot it will be considered as more or less autonomous. The scope of its autonomy is introduced by the manufacturer. See Bertolini, A. "Robots as products: The Case for a Real Analysis of Robotic Applications and Liability Rules", 2013) 5(2) LIT pp. 221-224

[37] See Sullins, J. "When is a robot a moral agent?" International Review of Information Ethics: Ethics in Robotics; Vol. 6 (12/2006) p. 26.

[38] *See* Darling, K. Op. Cit. p. 12. Where the author argues that robots rights should not only be considered depending on the moral obligations of those entities but in analogy with animals, due to the consideration that humans have on these entities, ("...Assuming that our society wants to protect animals regardless of their capacities, because of our personal attachments to them, society may well also want to protect social robots regardless of their capacities...").

[39] Sullins suggests that to allocate morality we must ask three questions: Is the robot significantly autonomous? Is the robot's behaviour intentional? Is the robot in a position of responsibility? *See* Sullins, J. "When is a robot a moral agent?" International Review of Information Ethics: Ethics in Robotics; Vol. 6 (12/2006) p. 26.

[40] *See* Stanford Enciclopediae, moral beings have "some degree for entity's own sake, such that it can be wronged" Nevertheless, moral status is graded but many authors that reserve Full Moral Status to human beings. Available at: http://plato.stanford.edu/entries/grounds-moral-status/ (Last Access: july 4, 11:04 am).

correlative features. However, moral reasoning is an uncertain possibility in robotics and it should be considered as hypothesis. In this sense, an approach to robots structure or capacities could eventually create doubts on the allocation of moral rights. For instance, if we consider the structure of the *brain*, i.e. the software embodiement of a robot (based on, e.g., the Multi Electrode Array[42]), there is no room for robot discrimination if we attend to the number of connections of both brains (independently of their natural or artificial origin)[43]. Moreover, if we consider determining morality based on robotic consciousness through the Turing test[44], we should also accept the possibility of denying rights to humans not passing that test[45]. It does not seem an intelligent solution[46].

So, if not granting moral rights to robots, other scenarios must be designed as a matter of urgency due to the impact that this technology is having on human beings[47]. Some authors suggest creating a new category of person. To say, the e-person: an entity to allocate special rights and duties to robots[48]. Yet the rights allocated to robots will be diluted by the fact there is no moral personality in them, the creation of a new category settles a wide space for future development of legal provisions concerning all topics relating robotic personhood. By contrast, as long as robotics primarily concerns with general matters such as kinematics, dynamics, path planning, and low level control issues, we could only refer to agenthood of the robot[49]. However, *de novo* status is a futuristic discussion and it may be inefficient for what the academia intends to achieve, which is no other than a legal frame for the industry and users.

---

[41] *See* Coeckelbergh, M. (2010) "Moral appearances: emotions, robots and human morality" Springer Science+Business Media B.V. 2010 pp. 240.

[42] *See* Coackelbergh, M. Op. Cit. p. 225 ("...The array measures 49mm x 49mm x 1mm and its electrodes provide a bidirectional link between the culture and the rest of the system ... It is estimated that each culture employed consists of 100,000 neurons").

[43] Coackelbergh suggests that the robotic brain could achieve the equivalent to 60 billion brain cells, despite the present characteristics of a "typical [robotic] brain...,splayed out on a 2-Dimensional array, contains around 100,000 neurons". *Op. Cit*. p. 223.

[44] Eugene Goostman, a computer created by PrincetonAI, has passed the 33.3% Turing Test threshold set by Alan Turing to consider it as a conscious being.

[45] *See* Coacklebergh, M. Op. Cit, p. 229.

[46] Traditional discussions about the nature of the autonomy of the robot, and the consequent allocation of rights based on the same autonomy is insufficient because the academy has incorrectly associated the reason why human beings have human rights is autonomy. However, the human being receives moral rights for the simple fact of being. Then we should assess the characteristics of the human, and if these are extrapolated to analogous entities (to say, of analogous humanity). For a further discussion see International Review of Information Ethics: Ethics in Robotics; Vol. 6 (12/2006).

[47] Analogous to the human-animal relationship, considering the robot as a positive element for human life, is the enhancer to create a new category. See our desire to protect animals from harm may not necessarily be based on their inherent attributes, but rather on the projection of ourselves onto these animals. See Darling, K. "Second order rights: Understanding Social Robots", in: The Second International Conferences on Advances in Computer-Human Interactions (ACHI). Cancun, Mexico.

[48] The reason by which we should avoid granting human analogous rights to robots (i.e. allocating human personhood) is, among others, that the decision of a robots is (and should be) always framed in a predetermined context by the manufacturer. The decision to be taken by the robot then lies in the frame coded by the manufacturer in the software of the robot. That frame is to be created in a certain context, predicted by manufacturer. See Bertolini, A. "Robots as products: The Case for a Real Analysis of Robotic Applications and Liability Rules", 2013) 5(2) LIT 214–247.

[49] *See* Weld, D.; Etzioni, O. "The firs Law of Robotics (a call to arms)", Department of Computer Science and Engineering, University of Washington.

III. REGULATION IN EUROPE

The doctrinal discussion of the role of the robot in society has opened the door to a possible specific regulation on the matter. In the context of a specific regulation, scholars have suggested two areas for a legal frame of robotics: (i) technical requirements or security standards in order to secure society from possible harms and (ii) reconsider legal liability that derivate from a robotic harm. In any case, European regulation shall gather up some leadership in robotics and translate it into a specific regulation. Relatedly, the discussion whether robotics requires of a specific regulation besides general cyberlaw[50] has found in the European RoboLaw Project and the euRobotics Coordination Action[51], an area of open discussion for the different stakeholders. The initiative was created by the European Commission to boost development of Robotics regulation in Europe. Nonetheless, applicable regulation can be already found in EU legislation and does not need of new ruling in major aspects, yet it is not condensed in a specific body of laws. However, its dispersion over a bunch of Directives, decisions and other legal instruments concerning software, electronic, information society, and general cyber laws could certainly create an uncomfortable legal environment for Robotics manufacturers and users[52] [53].

After all, basic principles should be established, starting with definitions. Despite the efforts to achieve consensus on the definition of 'robot', the ideas behind the existing literature[54] show that the definition should be established according to (i) International Standards[55], (ii) complex descriptions[56] or (iii) the identification of the common features of robotics; leaving aside exhaustive characteristics that would lead to an inefficient definition.

First option is acceptable as an International Standard, still, its introduction into an European law would need to include European specifications. Secondly, an exhaustive definition does not seem an efficient option for narrowing the topic as every robot would need of a detailed description on its particularities. It is therefore an illusionary possibility[57]. Finally, a definition

---

[50] *See* Calo, R. "Robotics and the New Cyberlaw" (February 28, 2014). California Law Review, Vol. 103, 2015. Available at SSRN: http://ssrn.com/abstract=2402972.

[51] Robolaw Project and euRobotics Coordination Action have been financed by the European Commission under the 7th Framework Programme.

[52] Applicable laws are: Directive 2006/42 on Machinery, Directive 2001/95 on General Product Safety (commercial guarantee), Directive 2001/29/EC of Information Society, 2004/48/EC on IP Enforcement, Directive 96/9/EC on Databases, Directive 2006/116/EC Term of Protection of Copyrights (2006), Directive 2011/77/ EC Term of Protection of Copyrights (2011), 2009/24/EC Software Directive, Directive 93/83/EC SatCab Directive.

[53] International regulation is also applicable to all Member States. Some of these international provisions are: Agreement on Trade-related aspects of IPR (TRIPS), Berne convention for the protection of literary and artistic works, UNESCO Copyright convention, WIPO Copyright Treaty as well as International standards such as EN ISO 10218-1:2008 for robots for industrial environments; and ISO 10218.1:2006/2011, for safeguard and restricted space.

[54] *Id.*

[55] *See* supra note 1 on ISO 8373.

[56] For instance, kinematics of a robot could be defined as $R = {}^{0}L6 = {}^{0}L1\,{}^{1}L2\,{}^{2}L3\,{}^{3}L4\,{}^{4}L5\,{}^{5}L6$ where ${}^{0}L1$ represents the position and orientation of the first link relative to the base reference; but this language could be too specific for a new legislation. *See* Zaldívar, D. "A Biped Robot Design", Department of Mathematics and Computer Science, Freie Universität Berlin, 2006, p. 70.

[57] Similarly to the impossibility to generate an exhaustive definition of "robot" is what happens with privacy by design; the interminable types of designs make a precise regulation unaffordable. For a deeper explanation *see*,

identifying the main features would be a practical approach as it would become a more flexible legislation, needed for the development stage of these technologies. Nonetheless, ISO 8373 already gathers up general features[58]. Hence, a fourth option would need to mix the International Standard with European references. This means an intermediate solution that gathers up two of the three previous positions. The new legal definition would read as follows:

> *A robot is an actuated mechanism programmable in two or more axes with a degree of autonomy [or emergence], to perform intended tasks and learn from the surrounding environment for use in industrial automation applications or that performs tasks for humans, in compliance with the European legislation.*

Another principle on which robotic regulation should be based is *liability*. The aforementioned projects have not been able to provide a clear solution for one of their intended purposes: to save social benefits by reducing the impact of product liability on the manufacturer. In this regard, it has been proposed to (i) flexibilize producer responsibility through a new regulation, (ii) to design a no-fault system, (iii) or even to create an agency borne by producers and users to provide compensation in the event of a damage.

From the wording of the Guidelines it can be inferred that there is a clear intention to amend the existing regulations so as to accommodate the interests of the industry. It is assumed that robotics is beneficial *per se* and it is also emphasized that priority should be given to adoption of such technology from ethical and moral principles. In the same vein, it has been suggested that an effort should be done in order to satisfy industry interests as well as it has been professed that these interests do not collide with social interests. An assumption that is perhaps too bold. As previously mentioned, authors generally agree on the need to apply technological advances to social development, but have rarely deepened on how to achieve such development; perhaps due to the lack of knowledge or to their excessive prudence. Therefore, we must insist on which base technology should be reinforced before getting into practical applications that robotic technology may have in the future. To construct a building where everyone fits, the foundations must be of unquestioned solidity.

Well, the *base* technology can again be divided in two: open and closed. This is essential since on the one hand, (i) one and other technology have radically different implications because one is based on the exclusive exploitation of the creations and the other in the culture of sharing. On the other hand (ii) limited liability of the robotics producer, to which many authors refer, already exists for open developers and producers while the weight of the responsibility of the closed robotics industry continues on the backs of the manufacturer.

IV. LIABILITY

e.g., Koops, B.J.; Leenes, R. "Privacy regulation cannot be hardcoded. A critical comment on the 'privacy by design' provision in data-protection law", International Review of Law, Computers & Technology, 2013.

[58] *See* supra note 1.

The lack of protection under moral rights make robots fall within the regulation of products, since its main characteristics[59] match those of any other product and can be object of trade. As to other software and hardware, robots are object of contract between manufacturers and end-users. Thus, two kinds of liability emerge from this frame: contractual[60] and non-contractual[61].

We are interested in the liability around what a robot *really* is: the conjunction of software and hardware that produces a 'repeated process of selective reproduction, random mutation and genetic recombination'[62]. These and previously mentioned features complicate the allocation of responsibility for damage[63] that cannot be directly attributed to the robot due to its dependence on its creator or on the user[64]. But, on the other side, learning ability and system complexity removes absolute control over the outcome of the product from the manufacturer (or programmer).

Despite the different circumstances that create an appearance of a responsibility gap[65], manufacturer is, indeed, the origin of the new *ens*. As a creator decides the extent to which a robot will function (the boundaries of its autonomy) but also the completeness of safety tests. Moreover, safety will somehow determine the success of technological products among end-users to whom some robots are intended[66]. Notwithstanding the producers' own criteria, it is reasonable to establish certain safety legal standards to the manufacturer[67] while they may also help when determining diligence employed by the manufacturer at the time to analyze the cause of the damage. However, the complexity[68] of the attribution of responsibility increases depending on whether the robot is based on an open or packaged system[69].

---

[59] Robots are designed, manufactured and programmed intending to enter the market for consumer use in response to their needs, with the inherent income arising from their sale.

[60] Lack of compliance with safety requirements may mean a violation of Article 1:301 of the Principles of European Contract Law, concerning "non-performance" of the contract. For that reason, safety measures set the benchmark for possible contractual responsibilities.

[61] Contractual liability concerns for the situations comprised by the license -e.g. system vulnerabilities-) and non-contractual liability comprises for situations such as injury to third parties). Although the contractual relation sets the frame for the claim, plaintiff can extend its demands under the protection of tort law. *See* Vihul, L. "The Liability of Software Manufacturers for defective products", The Tallinn Papers, Nato CCD COE Publication on Strategic Cyber Security, Vol.1, No.2, 2014.

[62] *See* Nolfi,S.; Floreano, D. "Evolutionary Robotics: The Biology, Intelligence, and Technology of Self-Organizing Machines" (MIT Press/Bradford, Cam- bridge 2000) quoted by Bertolini, 2013.

[63] *See* Marino, D.; Tamburrini, G. "Learning Robots and Human Responsibility" International Review of Information Ethics: Ethics in Robotics; Vol. 6 (12/2006) p 46-51. ('...Responsibility ascription problems in delegacy and trust in multi-agent systems are significant...').

[64] Scholars have distinguished between strong and weak autonomy. Depending on the extent of the decision making capacity of the robot it will be considered as more or less autonomous. The scope of its autonomy is introduced by the manufacturer. *See* Bertolini, A. "Robots as products: The Case for a Real Analysis of Robotic Applications and Liability Rules", 2013) 5(2) LIT pp. 221-224.

[65] Matthias identifies four points at which said gap is based. For the author, there is no enough information to predict what a learning robot will do in normal operating environments and select a course of action, (ii) there is no full control of the causal chain, (iii) as there is no control there cannot be any causal chain, (iv) the responsibility gap cannot be bridged by traditional concepts of responsibility adscription. *See* Matthias, A. "The responsibility gap: ascribing responsibility for the actions of learning automata", Kluwer Academic Publishers, the Netherlands, 2004.,

[66] *See* infra Part IV.2.

[67] *See* Leroux et al., Op. Cit., 2012.

[68] Scholars have questioned themselves whether special status and law should be created for robots, differentiating from the existing provisions in cyberlaw that would also. This is reasonable if we understand that functionality of robotics can have physical impact in society, while present cyberlaw does not consider the

A. Liability in close robotics

We must distinguish again between the two main types of liability: contractual and non-contractual[70]. The former is based on free market and established relationships between private parties by license or contract. To consider the manufacturer as responsible, there must be an absence of compliance with the agreed terms what would lead to the non-performance[71] of the contract. Thus, any harm occurred under the license agreement coverage should be considered as contractual liability. However, non-contractual liability introduces tastiest issues that can be divided in two scenarios: (i) harm caused by defective robot or (ii) harm caused by action or reaction of the robot in a human environment.

As regards the first scenario (i), EU legislation must be addressed to understand the scope of the concept of 'product'. In this sense, the 85/347/EEC Directive on Defective Products, understands the word 'product' as *all movables*[72]. This applies to the conjunction between software and hardware and, therefore, to robots[73], which are introduced to the market by the producer[74] through the aforementioned licensing agreement[75]. Indeed, the directive introduces strict liability as the mechanism to allocate responsibility on the producer or the importer[76] of a defective product[77]. Strict liability is generally applicable to areas where risks are high[78], so that the potential source of the damage makes all possible efforts to avoid the existence of damage. Its main feature is that responsibility is derived from the mere product defect, even if the producer has used sufficient diligence, by compliance with legal or

---

interaction between human and machines, this is, an interaction coming from both sides of the relation. The new regulation could be a facilitator for the different stakeholders in order to clarify its rights and duties, but this option is inconsistent with an adaptation of the existent legal provisions. *See* supra Part III.

[69] Due to the relevance of both types of system, the present paper analyzes both open and closed robotics liability in Europe; notwithstanding references to doctrine in other jurisdictions.

[70] As to any other product, robots are likely to be introduced in the market and be subject matter in a contract between the manufacturer and consumer. For further explanation on contractual and non-contractual liability in robotics *see* Leroux, C. et Al *Op. Cit*. 2012.

[71] Article 1:301 PECL: Non-performance is "...any failure to perform an obligation under the contract whether or not excused, and includes delayed performance, defective performance and failure to co-operate in order to give full effect to the contract...".

[72] Article 2 of the 85/374/EEC Directive.

[73] Directive 1999/34/EC amended 85/374/EEC Directive and it redefined the term 'product' as all movables even if incorporated into another movable or into an immovable.

[74] Article 3 of the 85/374/EEC Directive defines producer as the "...manufacturer of a finished product, the producer of any raw material or the manufacturer of a component part and any person who, by putting his name, trade mark or other distinguishing feature on the product presents himself as its producer...".

[75] According to Vihul these license agreements "...Tend to shield developers from most liability with respect to end-users who purchase their "shrink-wrapped" off-the-shield products, thereby down-streaming risk...".

[76] Strict liability is only imposed on manufacturers and importers (see Vihul, L.) whilst US' Strict Liability is imposed on manufacturers, distributors, and lessors of personal property and on builder-vendors of real property *See* Love, J. "Landlord's Liability for Defective Premises: Caveat Lessee, Negligence, or Strict Liability", Santa Clara Law Digital Commons, 1975.

[77] Defective product is defined by Article 6 of the 85/374/ECC Directive as the one not providing the safety which a person is entitled to expect. Member States have similarly introduced this definition in the National systems, for an excellent analysis on product liability and other issues concerning cyberlaw in Spain *see* Letai, P. "Cyber Law in Spain", Wolters Kluwer, Law & Business, 2nd ed.,2014.

[78] Main sectors where this theory applies are: traffic accidents, public administration, animals, hunting, nuclear energy, environment air navigation, defective products, proprietary liability. *See* Maddox, J. "Products liability in Europe: Towards a Regime of Strict Liability", 19 Journal of World Trade, Issue 5, pp. 508-201.

industry's[79] common practices. Consequently, the robot manufacturer will be declared as responsible when the tortfeasor has established causation between its conduct and the harm suffered by the victim[80], independently of the fault or negligence of the deceased[81].

But learning robots introduce other questions, as robotic growing abilities poke a future of unpredictability of robot behavior[82]. It has been suggested to equate robot's unpredictability to the status of the animal or the child[83]. For that reason, different parties involved in the robot learning process could be held liable according to the general rule of causation[84]. Their role in the product development and design is essential as they have the ability to modify the behavior of the robot from its early development to its full operability[85]. Nonetheless, it seems more appropriate that the learning period is carried out under the supervision of the programmer, who knows the implicit risks in the robot. This will prevent delegating learning tasks to unskilled users and to increase the predictability of robot behavior. To equate this situation to an existing context, we should refer to dogs for the blind[86] rather than to child or common animals. Accordingly, during the training period the manufacturer will be accountable for the damages caused by employees and representatives (i.e. trainers/teachers) under its supervision, as strict liability is also applicable in this context. Subsequently, law provisions should forbid introducing robots in the market without a complete training period where both the manufacturer and the end-user know the operating limits of the robot, which determines de *acceptable level of risk.* Therefore two sources of strict liability are identified in the robot manufacturer's side: (a) potential defective robots and (b) employee damages (robot harm during supervision).

Without prejudice to the responsibility so far analyzed, damage the robot may also involve responsibility outside the sphere of the manufacturer (including the teacher). That is, the area corresponding to the end user (ii). Producers are not held liable when the end-user makes a fault so that robot harmful behavior could be the consequence of either a product defect or the consumer fault[87]. But limits for manufacturer liability are not constrained to the wrongful consumer behavior and they are also given by the end-user risk assumption. The end-user should be informed by the risks and side effects of a robot (just like risk products such as pharmaceutical products) and, therefore, assume all consequences that could derivate from the use of the robot. Once the information has been delivered, the end-user is forced to care about robot behavior and follow instructions delivered by the manufacturer. Consumer should assume all risks concerning robots operability and follow the manufacturer's

[79] As established by american case law average care is not sufficient to exclude liability. There are precautions so imperative that even their universal disregard will not excuse their omission. See Eastern Transportation Co. (The TJ Hooper).
[80] Article 4 of the 85/374/EEC Directive.
[81] In Spain, like in most of European jurisdictions, Article 135 Royal Decree 1/2007 matches with European legislation and places the burden of proof on the victim. The existence of care will not be sufficient for the exoneration of the manufacturer. For further explanation on spanish tort law see Seuba, J.C. "Els elements de la responsabilitat civil (II): La imputació subjectiva de responsabilitat (negligència enfront de responsabilitat objectiva)", (Catalan) Universitat Oberta de Catalunya, p. 19.
[82] *See* supra, Part I.
[83] *See* supra Leroux et al. *Op. Cit*, 2012.
[84] Article 4:101 ECC.
[85] *See* supra note 6.
[86] *See* Bertolini, supra note 36.
[87] *See* Bergkamp, L.; Hunter, R. "Should Europe's Product Liability Regime Be Expanded? Comments on the European Commission's Green Paper on Product Liability" Analysis&Perspective, Vol. 29, No. 17, pp. 403-417.

instructions to the smallest detail. So, in case damage occurs, information can be tracked and the cause of the malfunction or error that causes the damage be determined.

Even though we have analyzed the main characteristics in product liability, we should note that European legislation introduces a flexible criterion for strict liability through exceptions[88] of Article 7 of the 85/374/EEC: among other provisions, it establishes that there is no liability if the manufacturer proves compliance with the existent regulation issued by public authorities or that the state-of-the-art at the time when the robot is put into circulation is not sufficient to allow the discovery of the defect[89]. Thus, these two provisions are most likely to protect close-robotics manufacturer against massive damage claims that could jeopardize a deep technology development by disincentivizing robotic massification.

B. Boosting shared development: liability in open robotics

As it has been said, robots are covered by product liability, and limits to manufacturer's liability should be found therein. Nevertheless, open-robots developers need of additional protection mainly due to social benefits that should be secured by the law. As discussed in the case of close-robotics, there is a risk that regulation put too great a weight on producer responsibility. Nonetheless, transmission of information around the risks of the robot and the modes of use may decrease manufacturer liability cases. Moreover, damages occurred outside the coverage of the license might be considered as end-user misuse. In fact, predetermined functionality settles the boundaries for manufacturer liability. Also, security required by the market represents itself an incentive for the manufacturer to create shrink-wrapped functionalities that permit to control the results of its products. But these assumptions are not applicable to open-robotics as this category of robots presents a wide amount of unclearness concerning liability, due to the latter development by the end user and the possible consideration of the open-product as a complement. This may lead manufacturers, investors and designers to reject that type of robotics[90]. The critic situation needs a development and new proposals of liability in open-robotics due to the social, economic and ethical importance of the open development of robotics[91].

Even so, some embryonic licensing development can be glimpsed in the open-robotics sector. The industry has developed licensing projects responding to the need to clearly convey responsibilities and rights to the end-user[92]. Additionally, general Open Source licenses are also applicable to robotics; for instance, the ROS project recommends coders and developers using the BSD licenses[93]. Commonly, as OR are created with the aim of facilitate information

[88] It was an optional clause; however, most EU Member States have chosen to incorporate it into their system.
[89] Article 7 (d),(e) of the 85/374/ECC Directive: "(d) that the defect is due to compliance of the product with mandatory regulations issued by the public authorities; or (e) that the state of scientific and technical knowledge at the time when he put the product into circulation was not such as to enable the existence of the defect to be discovered".
[90] Calo, R., "Open Robotics" Maryland Law Review, Vol. 70, No. 3, 2011. pp. 101-142.
[91] In the European context few projects have been started in the field of open-source robotics such as e-puck or iCub - an "open source cognitive humanoid"- (http://www.icub.org Last access: 11th January 2014).
[92] *See* Robotic Open Software Foundation: www.ros.org.
[93] *See* Darling, K. *Op. Cit.* p. 12. Where the author argues that robots rights should not only be considered depending on the moral obligations of those entities but in analogy with animals, due to the consideration that humans have on these entities, ("...Assuming that our society wants to protect animals regardless of their

to society with higher reliability, flexibility and lower cost, licenses impose little restrictions to redistribution.

As it can be inferred from the wording of the license[94], the primitive developer rests protected from any potential liability. Thus, it can be expected that the only likely liability to be imposed to the developer is due to non-performance[95] of the license (yet it might seem fictional possibility). Despite the protection with which the BSD license wants to provide the manufacturer, learning robots can complicate the allocation of responsibility. Hence, if the source code of the robot has produced the harm, the primitive developer could be held liable for introducing a harmful product into the market. But responsibility for the initial developer could be, at least, disproportionate and both economic and legal reasoning opt for disproportion of such measures. Notwithstanding this affirmation, robotics creates new scenarios that alter traditional schemes of tort law: entitlement transmission is compensated with liability rules, covering the potential harms that the acquired object might create. Nevertheless, the protection is constrained to the terms of the contract (or license) of transmission, which should undoubtedly include the most unclear feature of the robot: the extent of the learning process. Whilst it has been said that the learning process in close-robotics should be held under supervision of the manufacturer, open robotics poke an additional challenge. This is, the role of the user as developer.

This is where paths diverge. The unclearness of the license concerning potential harms to occur due to learned abilities cannot be equated to dogs for the blind. The open-robot building and learning process is totally led by the user. Therefore the robot rests outside the sphere of control[96] of the primitive developer and risks cannot be solely attributed to him. Causal link is likely to be derived from end-user inputs introduced into the robot. Nonetheless, each case has its peculiarities that do not allow generalizing this last statement. For that reason, when facing harm claims, courts will have to assess the different risks taken by manufacturer and the end-user of an open-robot.

Then, which is the solution for the open-robotic industry? First of all, existing regulation in Europe allows excluding open-robotic industry from liability. This provision is found in Article 7 of the 85/374/EEC Directive[97], by excluding manufacturers from liability when they prove that there was no economic intention in manufacturing the robot; so, this provision should apply if there is no sale related to license.

Besides full open-robots, robotic manufacturers in the open economy can introduce other kind of robotic applications. For instance, the Italian manufacturer Arduino, is delivering an

---

capacities, because of our personal attachments to them, society may well also want to protect social robots regardless of their capacities...").

[94] The ROS license reads: *"...in no event shall the copyright holder or contributors be liable for any direct, indirect, incidental, special, exemplary or consequential damages (including, but not limited to, procurement of substitute goods or services; loss of use, data, or profits; or business interruption) however caused and on any theory of liability, whether in contract, strict liability or tort (including negligence or otherwise)".*

[95] *See* supra Leroux, et al. *Op. Cit*, 2014, p. 53.

[96] In civil law, the liability will exist where there is an objective event (harm, causal link and specific action), unlawfulness of the action and fault.

[97] Article 7 (c) of the 85/374/EEC Directive establishes that "...The producer shall not be liable as a result of this Directive if he proves: [...] that the product was neither manufactured by him for sale or any form of distribution for economic purpose nor manufactured or distributed by him in the course of his business...".

undeveloped robotic platform called ArduinoStarterKit[98] where the user is able to build its own robot. Thus, this application could be considered as a component. European legislation establishes that in the case of a manufacturer of a component, the manufacturer is excluded from liability when proving that the defect was not attributable to its component but to the design of the robot or the instructions to the final manufacturer[99]. In this context, no exhaustive instructions are delivered to the end-user as he or she is to be considered as the manufacturer.

Again, Courts must weigh the inputs generated both by the primitive manufacturer and the end-user. To this end, the whole product features can be highly influential when referring to exceptions. For example, the fact that the StarterKid delivered by Arduino is charged with a fee could automatically exclude application of Article 7 (c). Nevertheless, as it is literally a box of components, Article 7 (f) should apply; then, open-robotic industry finds protection under existing laws. Nevertheless, uncertainty could act as a disincentive for the industry, and society would lose an opportunity to boost shared knowledge.

Scholars have argued that legality has an entitlement capacity. In other words, it can adopt the role of arbitrator where there is a conflict between parties and decide which interests prevail[100]. For that reason, different jurisdictions should also start initiatives in the field of robotic non-contractual harms, and, especially in the field of open-robotics due to its social relevance. Consequently, lawgivers should take a position on the topic in a specific regulation or leave to courts the task to set up solid case law and play an active role when establishing the boundaries to the industry. That is, open-robotics industry needs protection in order to generate shared information and access to robots without assuming the risks of creating potential semi-conscious beings that could negatively affect society depending on the abilities that the end-user has coded on its product without having any control on the end-user.

At this point, authorities must assess whether the public interest lies in protecting the industry or consumers. According to economic efficiency[101], entitlement should be assigned weighing social benefits and social costs of this open-technology. If such analysis is not possible, or does not prove to be accurate enough, another way to assess the question is whether the whole social cost should be assumed by a certain party (i.e. manufacturer). This, in open-robotics case, is unreasonable to charge the creator due to the underlying nature of this technology. To say, open-robotics developer cannot assume the consequences of delivering to society a product whose functionality can be determined by the end-user. On the one hand, societal benefits are valuable both for social development (by, e.g., shortening technological divide) and for scientific purposes (e.g. peer review, low cost, etc.) On the other hand, potential risks should be assumed by society when receiving valuable information that allows everyone to create a robot with physical embodiment[102].

[98] More information available at http://arduino.cc/en/Main/ArduinoStarterKit.
[99] Article 7 (f) of the 85/374/EEC Directive.
[100] For an excellent analysis on the relevance of entitling the party that inputs biggest benefit to society *see* Calabresi, G.; Melamed, A. "Property Rules, Liability Rules, and Inalienability: One View of the Cathedral", Yale Law School.
[101] *See* supra Part II.I.
[102] *See* supra Part II.

If social benefits are assumed by the majority, majority should also accept the side-effects of that benefit; a benefit that would not have been acquired without the input of the manufacturer.

CONCLUSION

As it has been attempted to demonstrate, the benefits of intensive expansion of *open* technology would permit to foster robot presence in society. To this end, existing legislation is ready to fully incentivize robotics producers by encouraging them to share their achievements with society, especially in the application of Article 7 of the Defective Products Directive.

The same happened with the Internet: thanks to an open network millions of people are able to communicate, work with and develop their lives in a manner that would not have been possible if the creators would have kept it for them. They shared their invention with others. Sharing is beneficial to everyone, and Product Liability Directive did not forget it.

We already have the umbrella; we need only to open it.

FRANCK CONROY
SOUS LA SUPERVISION DE LAURENT CYTERMANN

L'encadrement du « big data » et la protection des droits fondamentaux

FRANCK CONROY, étudiant à l'École de droit de Sciences Po, master Droit économique, spécialité Droit public économique

LAURENT CYTERMANN, maître des requêtes au Conseil d'État, rédacteur du rapport « Le numérique et les droits fondamentaux »

RÉSUMÉ

La protection des données personnelles doit faire face aujourd'hui à une évolution des technologies du traitement des données informatiques, qui relevaient encore de la science-fiction il y a dix ans, à l'époque de l'entrée en vigueur de la loi du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel. Le « big data » constitue un tel changement d'échelle du traitement des données numériques qu'il s'impose à la protection des droits fondamentaux et remet en cause le fondement de cette protection.

INTRODUCTION

La chaîne américaine de supermarchés Target est l'objet d'un fait divers célèbre concernant le « *big data* ». L'analyse statistique d'un grand nombre de données numériques a permis à la chaîne de déterminer très précocement si une femme était tombée enceinte, notamment à travers les habitudes d'achat de femmes enceintes de trois mois payant par carte de crédit, ou par carte de fidélité. Selon les statistiques, une femme dans cette situation préférera, par exemple, les crèmes non parfumées et investira dans les compléments alimentaires peu de temps après. La chaîne de supermarchés peut alors en profiter pour fidéliser la future mère à de nouvelles marques et produits utiles à la maternité. L'analyse globale de paniers de clients après le recueil massif des données d'achat permettait, par ailleurs, de prédire assez précisément la date de l'accouchement. C'est ainsi que la publicité ciblée de Target, dont le

nom se traduit par « cible » en français, a révélé la grossesse d'une lycéenne à ses parents avant que ces derniers n'en soient informés ! Cette utilisation agressive de données numériques à caractère personnel est une illustration des pouvoirs prédictifs d'une telle analyse de données à grande échelle et de possibilité de valorisation conséquente.

Heureusement, le « *big data* » n'est qu'un outil, permettant des utilisations moins invasives et plus utiles à l'intérêt général. Mais l'exemple des supermarchés Target souligne certaines des problématiques mêlant droits fondamentaux et « *big data* ». Ces problématiques se cristallisent autour de plusieurs étapes du phénomène, notamment la collecte et l'utilisation de données numériques à caractère personnel.

Aujourd'hui, il existe pourtant un encadrement règlementaire efficace de l'utilisation des données numériques. Mais l'évolution rapide d'un nouveau genre d'exploitation de ces données fait émerger un nouveau défi pour la protection des droits fondamentaux des individus regardant les informations les concernant. Une question essentielle se présente à nos yeux : l'encadrement des données numériques est-il adapté au phénomène du « *big data* » ? La compréhension des différents aspects du phénomène (**I**) et une vue du cadre règlementaire actuel (**II**) sont nécessaires, pour réfléchir, ensuite, aux modalités existantes ou souhaitables d'encadrement (**III**) d'un phénomène tel qu'il promet de changer notre manière d'appréhender et résoudre les problèmes politiques ou commerciaux à venir.

I. LE « *BIG DATA* » EST UNE PROCÉDURE DE VALORISATION DE BANQUES MASSIVES DE DONNÉES NUMÉRIQUES

A. La nature et les utilisations du « *big data* »

La difficulté de se représenter tous les tenants du « *big data* » vient de ce que le concept regroupe une multitude de phénomènes qui forment partie de tout un processus de traitement d'informations. Une définition synthétique du « *big data* », pris comme un seul phénomène, serait « *ce qui peut être accompli à grande échelle et ne peut pas l'être à une échelle plus petite, en matière d'extraction de nouvelles connaissances ou de créations de nouvelles formes de valeur, avec comme impact la transformation des marchés* »[1]. Le « *big data* », à la lumière de cette définition, doit être étudié comme un phénomène uni puisque c'est dans cette unité que la collecte sert au traitement d'informations. Ce dernier sert, à son tour, aux prévisions ou aux analyses de grande échelle. Pourtant, ces divers éléments posent chacun leurs propres questions : la collecte d'information ne relève pas des mêmes problématiques que l'analyse. La formule des « 5V » est souvent reprise pour caractériser les différentes étapes du processus de collecte et d'utilisation du « *big data* » : volume (de la totalité des données collectées), variété (des données et des sources), vitesse (de l'analyse des données), véracité (qualité de l'analyse), valeur (créée à partir de l'analyse)[2]. Elle permet d'évaluer toutes les étapes du phénomène, du rassemblement de données à la valorisation finale des analyses produites à partir des données.

1. La collecte d'information

[1] K. CUKIER, V. MAYER-SCHÖNBERG, « *Big data : la révolution des données est en marche* », trad. H. DHIFALLAH, ed. Robert Laffont, Paris, 2014.
[2] Commission générale à la stratégie et à la prospective, « *Analyse des big data : quels usages, quels défis ?* » Note d'analyse n°08 de novembre 2013.

Le phénomène du « *big data* » s'est développé avec l'accroissement de la puissance informatique des processeurs. Il repose sur la capacité des ordinateurs à stocker et collecter des quantités titanesques de données, alors que cette capacité n'aurait pas été envisageable quelques années auparavant. Cette nouvelle puissance de calcul informatique a permis, en 2013, de conserver 98% de l'information stockée dans le monde sous forme numérique, alors que la forme numérique ne représentait qu'un quart des moyens de stockage de l'information en 2000[3]. Autre exemple de la multiplication de la capacité informatique : Google traite 24 pétaoctets[4] de données numériques chaque jour[5], ce qui aurait été impensable il y a dix ans. La donnée numérique a comme qualité de transformer toute information en un langage unique lisible par un ordinateur – le langage binaire – comme une requête sur un moteur de recherche, de la musique ou une image. Cette accumulation d'information en tout genre, dont on a cité quelques exemples à l'usage évident, mais qui regroupe aussi des informations, telles que les données recueillies par les senseurs d'une voiture sur la position du conducteur, ou les différents prix d'un billet d'avion. Il faut à ce propos différencier les données numériques en général, des données numériques permettant d'identifier une personne, qui relèvent de la protection accordée par les lois sur le numérique et la défense des libertés individuelles, notamment la loi « Informatique et libertés » de 1978, modifiée en 2004 en France, et dont nous étudierons la portée dans une deuxième partie.

Le phénomène du « *big data* » dépend en premier lieu d'un processus d'accumulation de données, rendu possible par une puissance de calcul des processeurs toujours plus importante. Ce qui donne son nom au phénomène c'est, en effet, le volume de données collectées par divers procédés qui ne sont pas nécessairement en relation évidente avec l'objet ou l'utilisation finale de ces données. Pourtant, la collecte et le stockage de données ne sont pas l'essence de la révolution du « *big data* » ; elle partage son rôle dans le « *big data* » avec la combinaison de diverses données, l'interprétation qui en est extraite et, enfin, l'utilisation des conclusions à laquelle le croisement des données permet de parvenir.

L'accumulation de données aussi disparates n'a aucun intérêt en soi, même si, comme on le verra plus loin, le phénomène de « *big data* » est, dès ce stade, régi par la protection des droits fondamentaux. Le bénéfice le plus important tiré de l'amélioration des capacités de calcul, outre la quantité de données stockées, c'est la possibilité d'en tirer des corrélations.

2. Le traitement d'information

Une corrélation est une mise en relation statistique. Une telle mise en relation suggère un lien fort entre deux valeurs si la modification d'une de ces valeurs s'accompagne fréquemment d'une variation de l'autre valeur. On ne peut tirer aucune certitude concernant la causalité de cette relation – la relation peut en effet tenir de la coïncidence ou de facteurs tierces non pris en compte. En revanche, un tel lien de corrélation peut avoir une valeur prédictive intéressante, qui est centrale à l'exploitation du *big data*. Le traitement des données accumulées permet de faire ressortir des corrélations utiles pour l'exploitant des informations : Amazon ou Walmart ont pu analyser l'intérêt que pourrait avoir un client pour un article après l'achat d'un premier article sur le site d'Amazon, ou la préférence d'un client

[3] *Ibid.*
[4] 10^{15} octets, « péta » correspond à un million de milliards.
[5] *Ibid.*

pour l'achat de « *Poptarts* » en fonction des prévisions d'ouragan[6]. La probabilité qu'un client achète un second article est corrélée à la variation d'une première donnée, que ce soit l'achat d'un livre ou une prévision météorologique.

L'exploitation des données peut conduire à des résultats tout à fait surprenants : Google a pu prédire, jusqu'en 2012, les épidémies grippales, en exploitant sa base de données de requêtes, selon un modèle mathématique concernant une cinquantaine de mots-clés[7]. C'est une utilisation vertueuse des données qui a intéressé les hôpitaux nécessitant un moyen de réagir rapidement à la propagation des grippes, et notamment à la possibilité de propagation du virus H1N1. À l'inverse, l'utilisation par les compagnies d'assurance de probabilités concernant les attaques cardiaques tirées de l'exploitation de « *big data* » n'est pas aussi réjouissante. La comparaison de ces deux exemples fait ressortir les enjeux juridiques et sociaux du « *big data* » : dans la myriade de possibilités d'utilisation du « *big data* », le phénomène ne se résume pas à la collecte de données mais à leur exploitation, qui peut n'avoir qu'un lien ténu avec les motifs initiaux de la collecte.

B. Les aspects litigieux du phénomène « *big data* »

1. Les inexactitudes

Les questions soulevées par les différentes composantes du phénomène lui-même s'accompagnent de problèmes liés à la nature du « *big data* ». En premier lieu, il s'agit fondamentalement de données et de corrélations, éléments pour lesquels l'incertitude joue un rôle essentiel. Une donnée « factuelle » peut ainsi être erronée ou inexacte, mais l'inexactitude des données se multiplie avec leur accumulation. D'une part, la probabilité que la base de données contienne des informations fausses croît avec la taille de la base. D'autre part, la quantité très importante de données peut elle-même être à l'origine d'erreurs, si ces données proviennent de sources différentes, ou si elles ne sont pas aussi fiables les unes que les autres, ce qui accroît l'incertitude quant à la fiabilité générale de la base. L'élimination de la causalité ou d'une interprétation humaine d'un résultat en faveur d'une corrélation « suffisamment » précise peut être tentante mais constituerait une faute d'appréciation grave à cause des risques d'erreur statistique suscités. Ainsi, ce qui semble n'être qu'une question statistique constitue néanmoins à la fois un risque – conclusions dangereuses tirés d'informations erronnées – et une menace pour la protection des droits fondamentaux – on oppose abondance et précision des données pour suivre une tendance générale.

2. La collecte de données à l'encontre de la confidentialité et du consentement

La collecte de ces données personnelles est l'un des aspects les plus médiatiques et les plus réglementés du « *big data* », notamment le conflit entre le droit au respect de la vie privée et la collecte de données permettant l'identification d'une personne. Le consentement à la collecte

[6] *Ibid.*, p.70.
[7] *Ibid.* p.10.

concilie, en principe, les deux aspects, mais n'est pas une solution entièrement satisfaisante dans la mesure où les sources et la nature des données personnelles en circulation sont de plus en plus variées : elles peuvent être collectées automatiquement (à travers les « *cookies* » par des sites Internet notamment) ou mises en ligne par la personne concernée elle-même sur un réseau social[8]. Le contrôle de tant d'informations et de données en circulation sur soi-même est rendu difficile par la quantité et la dispersion de l'information. Cela peut entraîner la diffusion de données à l'insu de l'usager concerné alors que leur collecte a été consentie dans un premier temps.

La collecte de données peut également devenir abusive si elle est utilisée à des fins de différenciation commerciale entre clients destinés à être plus ou moins pénalisés selon ce que leurs données révèlent. L'utilisation de messages personnalisés à partir de telles données peut tout simplement relever d'un « *préjudice d'agacement* »[9]. Or il s'ensuit de la logique économique que les bases de données les plus importantes permettent les analyses les plus complètes, et que la collecte devra se faire nécessairement de la manière la plus étendue possible. Ces problèmes n'ont trait qu'à des pratiques commerciales ou des services publics, mais il faut également souligner que la protection des droits fondamentaux cherche à prévenir les utilisations malveillantes des données (l'usurpation d'identité par exemple). C'est un phénomène accessoire au « *big data* », dans la mesure où il ne s'appuie pas sur la collecte d'un grand nombre de données, mais dans la dissémination des données encouragée par le « *big data* ».

Le principe de finalité déterminée des données s'oppose ainsi à la collecte indiscriminée des données. Le consentement au recueil de données passe en effet par l'utilisation faite des données. Or, il est possible qu'une utilisation bienveillante, mais découverte *a posteriori*, entre en conflit avec cette exigence. Plusieurs autres principes étudiés ultérieurement découlent du principe de finalité déterminée qui caractérise une des problématiques principales du « *big data* » : est-il compatible avec le respect du consentement d'une personne donné pour une certaine utilisation, de faire émerger des corrélations entre données collectées pour d'autres usages et venant de différentes sources ?

Le cadre règlementaire et jurisprudentiel européen et national définit les usages licites et illicites des données par traitement automatisé et tente de répondre à cette question.

C. Les données numériques font l'objet d'une réglementation très développée

Ces problématiques proviennent soit de la rencontre du « *big data* » avec la loi régissant les données numériques, soit des conséquences, jusqu'alors inconnues, issues des différents éléments du phénomène.

1. Le cadre juridique actuel concernant les données numériques

A l'origine, les données numériques étaient soumises, en France, à la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, dite loi « Informatique et libertés ».

[8] Conseil d'État, « *Étude annuelle 2014 du Conseil d'État - Le numérique et les droits fondamentaux* », La Documentation Française, septembre 2014, p.155.
[9] *Ibid.*, p.160.

La loi du 6 août 2004 constitue la seule grande réforme qu'elle ait subie, renouvelant ses définitions et le cadre juridique de la protection des données personnelles. Elle s'applique aujourd'hui « *aux traitements automatisés de données à caractère personnel, ainsi qu'aux traitements non automatisés de données à caractère personnel contenues ou appelées à figurer dans des fichiers, à l'exception des traitements mis en oeuvre pour l'exercice d'activités exclusivement personnelles, lorsque leur responsable remplit les conditions prévues à l'article 5* ». La loi du 6 janvier 1978 établit une définition importante et large pour les données à caractère personnel : « *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* ». A partir de cette définition, la loi « Informatique et libertés »[10] a construit un premier cadre de la protection des personnes et des données numériques en fondant la Commission nationale de l'informatique et des libertés (CNIL), et en établissant une protection large des données personnelles[11] et le droit des personnes de disposer dans une certaine mesure des données les concernant, dont le droit de consentir à la collecte de données à caractère personnel.

En Europe, le cadre de la régulation du domaine numérique dépend de plusieurs textes, dont un des premiers d'envergure est la Convention n°108 du 28 janvier 1981 du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel. Un des apports importants de la convention, en particulier pour les problématiques de droits fondamentaux concernant le « *big data* », est le principe de « qualités des données », duquel découlent le principe de loyauté de la collecte, ou encore le principe de finalité déterminée d'une collecte. On compte, également, le principe de proportionnalité de la collecte des données à ces finalités, le principe d'exactitude et le principe de limitation de la durée de conservation.

Ces principes ont été transposés en droit français par la loi du 6 août 2004, relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel. La loi a dû faire face aux grandes révolutions de l'informatique survenues, dans un premier temps, entre 1978 et 1995, avec le développement des ordinateurs et leur arrivée dans les entreprises et dans les foyers, puis entre 1995 et l'adoption de la loi, où l'informatique s'est largement popularisée. Les pratiques relatives à l'informatique ont naturellement évolué en conséquence, de telle sorte que la loi du 6 janvier 1978 ne permettait plus un contrôle efficace du traitement des données personnelles devenues beaucoup plus répandues et dispersées qu'elles ne pouvaient l'être en 1995. Ainsi, la loi du 6 août 2004 a mis à jour les pouvoirs et les fonctions de la CNIL. De fait, la distinction privée et publique de l'autorisation du traitement des données n'était plus adaptée à la réalité de l'utilisation massive de données informatiques. Avec la loi du 6 août 2004, la CNIL cesse d'être responsable de l'autorisation du traitement des données par le secteur public. Son contrôle porte désormais principalement sur le traitement privé des données par le secteur privé, dans la mesure où la distinction entre type de données porte sur la nature de la donnée et la sensibilité de l'information qu'elle porte, plutôt que sur

[10] Art. 2 de la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.
[11] Sont concernées par le chapitre II de la loi, sur les conditions de licéité des traitements des données à caractère personnel notamment les méthodes de traitement des données (le traitement de données faisant apparaître l'origine ethnique par exemple) ou encore les différentes finalités que peut avoir un traitement.

l'identité du traitant de la donnée. Certains types de données ne peuvent être recueillis, comme les données à caractère ethnique (article 8 de la loi du 6 janvier 1978 modifiée), alors que d'autres traitements sont soumis à autorisation, lorsque ces données ont un caractère sensible, comme les données génétiques, relatives à des infractions ou aux difficultés sociales rencontrées par une personne. Ce recentrement de l'activité de la CNIL accompagne ainsi l'évolution du traitement des données personnelles, aujourd'hui largement effectué par des acteurs privés[12]. La protection des droits fondamentaux doit donc porter, en priorité, sur cette activité privée de traitement commercial de données. L'activité publique demeure, néanmoins, sujette à certaines autorisations de traitement de données, comme pour le traitement de données relatives à la sécurité publique, par exemple. L'avis de la CNIL dispose d'une autorité particulière, seul un décret en Conseil d'État ou un arrêté ministériel pris après un avis de la CNIL peuvent autoriser un traitement de données sensibles

En résumé, le droit de l'Union et le droit national fournissent un cadre règlementaire et jurisprudentiel qui s'appuie à la fois sur l'usager ou la personne concernée, en se fondant sur son consentement et les conséquences qui en dérivent, comme l'accès aux données, la possibilité d'en disposer à la fois sur le détenteur, ou le collecteur des données, en soumettant le traitement des données à des conditions de collecte et de traitement respectueuses des libertés fondamentales. Cependant, la refonte du cadre est prévue par le paquet adopté par la Commission le 25 janvier 2012 sur la protection des données personnelles. Il inclut une proposition de règlement et de directive pour harmoniser le cadre européen, qui, de fait, se compose aujourd'hui de vingt-huit cadres nationaux et vingt-huit transpositions différentes de la directive du 24 octobre 1995.

2. L'application de ce cadre au « *big data* »

Ce cadre trouve donc à s'appliquer pour les banques de données relevant du « *big data* ». Or, nombre de ces principes entrent en contradiction avec la logique du « *big data* », comme nous avons pu le voir précédemment. Le Conseil d'État dans son rapport sur le numérique et les droits fondamentaux étudie tous les obstacles au développement du « *big data* » que peuvent constituer les principes issus de la Convention n°108 et la directive du 24 octobre 1995. Il est intéressant de les rappeler ici, puisqu'ils illustrent le décalage, ou plutôt le conflit de priorités, entre l'état actuel de la protection des droits fondamentaux et le développement du « *big data* ».

L'identification par les données personnelles

En principe, la détermination d'une donnée numérique en une donnée à caractère personnelle obéit à la définition large de la loi du 6 janvier 1978 et de la directive du 24 octobre 1995 transposée par la loi du 6 août 2004. En pratique, l'étendue de la définition laisse des frontières floues autour de ce qui pourrait caractériser une donnée permettant d'identifier une personne, comme les adresses IP[13]. De manière générale, une attitude protectrice est adoptée face à la

[12] Le *Rapport d'activité 2012*, paru en avril 2013, de la CNIL indique de 77% des plaintes portante sur la combinaison des secteurs « internet/télécoms », « commerce », « travail », et « banques ».
[13] CJUE, arrêt *Scarlet c/ SABAM*, C-70/10, 24 novembre 2011: les adresses IP constituent pour la Cour des données protégées à caractère personnel.

définition des données à caractère personnel. Une banque de données « *big data* », en revanche, peut tirer des données de différentes sources, qui n'ont parfois pas pour but initial d'identifier une personne, et dans une quantité telle que le caractère personnel des données peut être difficile à établir à cause du tri à opérer parmi ces données – c'est l'effet « boîte noire » des prédictions se fondant sur des algorithmes et une quantité de modèles mathématiques telle qu'on ne peut l'appréhender sans outils[14]. L'usage de ces données qui, à l'origine, ne relevaient pas d'un caractère personnel, peut aussi permettre d'identifier une personne selon la nouvelle utilisation découverte pour ces données.

Les principes découlant de la qualité des données

La qualité des données est un des principes fondateurs de la protection des droits fondamentaux. Il est inscrit à l'article 5 de la Convention n° 108, aux articles 6 de la loi du 6 janvier 1978 et à la directive du 24 octobre 1995, et même à l'article 8 de la Charte des droits fondamentaux de l'Union européenne. La loi du 6 août 2004 les porte en droit français en transposant la directive de 1995. Il en découle sept principes : le principe de finalité déterminées, le principe de proportionnalité – naturellement lié à la finalité d'une donnée pour évaluer la proportionnalité – le principe de pertinence des données, la limitation de la durée de conservation des données, le principe de sécurité et de confidentialité, le principe de transparence et le principe du respect des droits des personnes[15]. Le principe des finalités déterminées est l'un des principes les plus critiqués au regard des défenseurs du « *big data* » : la force du « *big data* » étant de trouver des utilisations innovantes – et par conséquent imprévues – à une masse de données disparates. On peut ainsi noter que l'article 32 de la loi du 6 janvier de 1978 modifiée maintient l'obligation d'établir une finalité à la collecte de données, même lorsqu'elles peuvent avoir un objet secondaire se rapportant à des activités d'intérêt général, telles que la recherche historique, statistique ou scientifique, de même, lorsque les données ont été rapidement rendues anonymes. La quantité de données employées est, elle-même, capitale et entre en contradiction avec le principe de proportionnalité, voire du principe de limitation de la durée de la conservation des données. Face au bénéfice de l'outil « *big data* », certains défenseurs de la cause du « *big data* » préconisent de déplacer le point de fixation de la protection des droits fondamentaux du consentement de l'individu vers la responsabilité de l'utilisateur des données. Ils proposent également un déplacement vers une procédure plus souple qui ne requiert pas d'autorisation, mais qui encadre *a posteriori* l'utilisation à mauvais escient des données[16].

Mais ces principes fondent la protection des droits fondamentaux des personnes. Tant l'approche européenne que l'approche étatsunienne[17] de la relation entre droits fondamentaux et données numériques font du consentement la clef de voûte de la protection des droits fondamentaux, en ce que le consentement fait le pont entre les différents droits appartenant à un individu, tels que le droit à l'information, le droit à la protection de sa vie privée et la collecte de données, qui constitue le point de départ du phénomène « *big data* ». Deux

[14] K. CUKIER, V. MAYER-SCHÖNBERG, « *Big data : la révolution des données est en marche* », *op. cit.*, p.217.
[15] « *Les 7 principes clés de la protection des données personnelles* », Correspondant Informatique et libertés du CNRS, Page publiée le 19 octobre 2011, mise à jour le 18 janvier 2012, consultée le 7 novembre 2014, http://www.cil.cnrs.fr/CIL/spip.php?article1390.
[16] K. CUKIER, V. MAYER-SCHÖNBERG, « *Big data : la révolution des données est en marche* », *op. cit.*, p. 214.
[17] Executive Office of the President, dir. J. PODESTA, « *Big Data: Seizing Opportunities, Preserving Values* », May 2014.

principes permettent de consentir à la transmission de données : le principe des finalités déterminées que nous avons étudié, et le principe de loyauté et d'exactitude, un principe qui permet d'entretenir la confiance d'un individu envers un collecteur de données et de donner par la suite son consentement. Dans son rapport, le Conseil d'État prend pour exemple l'utilisation des données par un moteur de recherche dans le cadre de l'amélioration de son service. Cet usage correspond à l'usage attendu par l'individu, qui y consent en se fiant au fait que le moteur de recherche n'ira pas ensuite revendre ces données à des acteurs déconnectés de son activité tels que des assurances. A l'inverse, la jurisprudence tend à réprimer la déloyauté dans le traitement de l'information[18]. Il faut insister sur l'importance de ces principes, parce qu'ils sont communs à la fois au cadre européen, mais aussi parce qu'ils déterminent la façon dont le contrôle s'exerce : on retrouve ainsi une opposition entre la focalisation sur le consentement de l'usager ou du sujet de l'information et la responsabilité des entreprises qui traitent ces données.

Les principes fondamentaux soutenant la protection des données personnelles sont donc partagés au niveau national et européen grâce à la transposition de la directive du 24 octobre 1995. Plusieurs évolutions sont en cours pour renforcer cette protection, notamment avec la proposition de règlement que nous avons évoquée précédemment. Les évolutions sont jurisprudentielles d'abord, avec l'arrêt de la CJUE *Google Spain c/ AEPD* du 13 mai 2014, par lequel les moteurs de recherche sont tenus pour responsables du traitement des données personnelles collectées. Les évolutions sont également législatives, avec le renforcement des principes par la proposition de règlement que nous étudierons plus avant dans cet article.

D. Quelle piste doit-on suivre pour l'encadrement du « *big data* » ?

1. Les conclusions à tirer du cadre actuel ?

Le cadre juridique actuel défend une position qui semble inadaptée au développement du « *big data* ». Ce cadre reste néanmoins plus protecteur que les propositions qui tendent à déplacer la focalisation de la protection des données numériques sur la responsabilité des utilisateurs des données. Plusieurs critiques s'attaquent à l'illusion du consentement face au retraitement des données, aux moyens de contournement tout à fait licites du consentement de l'individu concerné par les données, ou face à l'accord « forcé » qu'entraîne l'obligation de consentir à l'utilisation des données à caractère personnel pour accéder à un service ou simplement à une page Internet[19]. En somme, le consentement serait une façade et non l'expression de droits fondamentaux. Il faut reconnaître qu'une position intermédiaire peut être adoptée, dans la mesure où la quantité des données recueillies dans un cadre « *big data* », ou tout simplement la complexité des formulaires numériques de consentement, jettent un doute sur la capacité d'un individu à fournir un consentement. Le consentement est néanmoins le moyen le plus sûr d'application des principes énoncés plus haut. On ne peut oublier que la protection des données à caractère personnel a pour objet, avant tout, la défense de l'individu concerné.

Cependant, le cadre actuel est peut-être partiellement inadapté. On peut arguer que le rôle du juge et du législateur doit, avant tout, porter sur la défense des droits individuels. Les principes

[18] CE, 12 mars 2014, *Société Pages Jaunes Groupe*, n° 353193.
[19] H. NISSENBAUM, «*Privacy in Context: Technology, Policy, and the Integrity of Social Life* », Stanford University Press, 2010.

décrits ci-dessus, appliqués par les cours nationales et européennes, défendent, de fait, les droits fondamentaux des individus. Nous avons également vu que nombre de ces principes semblent s'opposer à plusieurs stades du processus de valorisation du « *big data* », alors que le « *big data* » se généralisera indépendamment de l'évolution du droit national. Le cadre actuel, s'il est encore adapté aujourd'hui à une protection efficace des droits fondamentaux, peut éventuellement être dépassé par l'évolution du phénomène.

Le parallèle entre cadres étatsunien et européen

Les premières mesures de protection des données informatiques et personnelles aux Etats-Unis sont prises en 1970, concernant le traitement de données bancaires, et en 1974, pour le traitement des données personnelles, le premier *Privacy Act*. Le 1er mai 2014, un rapport sur le «*big data* » est rendu au Président Obama, analysant les évolutions prévisibles de son utilisation et les mesures souhaitables de protection des données personnelles dans le cadre du « *big data* ». Le rapport pose quatre questions concernant la politique à adopter au regard du développement de ces technologies et du traitement des données impliquées : comment l'intérêt général peut-il bénéficier au « *big data* » à travers son utilisation par l'État tout en se gardant de porter atteinte aux intérêts des citoyens ? ; comment l'utilisation du « *big data* » transforme le paysage commercial au point d'impliquer des valeurs fondamentales dans le processus ? ; comment protéger les citoyens de prédictions comportementales abusives permises par les technologies du « *big data* » ? ; comment le « *big data* » affecte les principes fondamentaux de la protection de la vie privée, notamment les principes d'information et de consentement ? Le rapport soulève un point intéressant du contrôle des données personnelles : le développement des technologies de renforcement de la protection de la vie privée et notamment le financement gouvernemental de cette recherche. Ces technologies incluent des techniques d'anonymisation et de limitation de la collecte d'information. C'est une piste intéressante à explorer dans la mesure où le traitement des données personnelles est, avant tout, une question dont les réponses sont tant juridiques que technologiques, et peuvent apporter des moyens de renforcer le cadre juridique et le consentement de la personne concernée par le traitement de ses données personnelles.

La protection des données personnelles aux Etats-Unis oscille également entre la protection fondamentale du consentement et le besoin économique des entreprises utilisant ces données pour une plus grande flexibilité du processus de traitement, qui exigerait une protection fondée plutôt sur une utilisation responsable de ces données. Cette équation se retrouve donc entre Europe et États-Unis, dans la mesure où l'anticipation des évolutions du « *big data* » est un enjeu majeur pour le cadre juridique de protection des données personnelles.

La protection des données personnelles aux États-Unis n'est pas unifiée comme elle l'est en France. Le cadre juridique étatsunien établit une protection des données selon le secteur d'activité concerné, fondée sur des lois de niveau fédéral et étatique. Les deux échelons sont ainsi chargés d'assurer le respect des lois de protection des données personnelles, tandis que ces mêmes lois permettent au citoyen d'agir en justice contre une société ou une organisation qui aurait enfreint une telle loi[20]. Il se caractérise, ainsi, par la réparation des dommages subis, plutôt que la prévention des atteintes à la vie privée que privilégie l'Union européenne.

[20] « United States », L. SOTTO, A. SIMPSON, « *Getting the Deal Through: data protection and privacy in 26 jurisdictions worldwide* », ed. Law Business Research, London, 2014.

Partant, il faut aussi souligner l'absence de régulateur centralisé. Les préoccupations et les principes gouvernant la protection des données personnelles sont donc similaires entre l'Union européenne et les États-Unis ; on peut à ce sujet se référer aux divers accords qui régissent la coopération en matière de transfert de données tels que la procédure « *Safe harbour* » pour les entreprises américaines, mais les instruments pour appliquer ces principes sont au contraire très différents, ce qui peut constituer un danger compte tenu de la nature très fluide des données informatiques. Une renégociation de la procédure « *Safe harbour* » est en cours[21]. On observe en même temps un rapprochement mutuel des pratiques à travers un « *Brussels effect* », une influence des mesures de régulation européennes, notamment en matière de protection de données, sur les normes de pays tiers, dont les États-Unis[22].

L'influence réciproque des cadres européens et étatsuniens apparaît également dans la refonte prochaine du cadre européen de la protection des données. Un règlement sur la protection des données personnelles est appelé à remplacer la directive du 24 octobre 1995, notamment en vue d'harmoniser les législations nationales sur la protection des données, et pour mieux faire face au caractère transnational d'Internet et du « *big data* », à la fois au sein des frontières européennes et avec les États tiers. Le règlement s'accompagne d'une directive plus spécifique sur la protection des données personnelles « *traitées à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière, ainsi que d'activités judiciaires connexes* ». Le paquet comprenant le règlement et la directive a été adopté par le Parlement européen le 12 mars 2014. En particulier, il établirait une autorisation préalable obligatoire pour le transfert de données d'une société à un État tiers de l'Union européenne, et plus généralement une responsabilisation accrue des sociétés traitant un grand nombre de données : la nomination d'un « *data protection officer* » par exemple, mais aussi l'ajout d'un dernier principe relatif à la protection des données, celui de la charge reposant sur la société de traitement de prouver la conformité de son traitement de données. Le règlement a également pour objectif de centraliser le contrôle des données en Europe. Les sociétés n'auraient alors plus qu'un interlocuteur, l'autorité nationale de l'État où se trouve leur établissement principal, à laquelle les citoyens auraient aussi accès. Il est à noter que le règlement réaffirme les principes encadrant la protection des données. Partant, le consentement explicite à la transmission de ces derniers demeure, dans le règlement, la pierre angulaire de la récolte et du traitement de données personnelles[23].

2. Quel encadrement privilégier ?

Sans nuire à la protection que les principes susmentionnés fournissent, un objectif nécessaire sera donc d'adapter soit leur forme, soit les instruments d'application de ces principes à l'avènement de la société d'information prévue par la stratégie Europe 2020, ou plus simplement à la croissance de la puissance informatique et à la généralisation des procédés s'appuyant sur la collecte massive de données numériques. Parmi ces instruments, on peut compter les méthodes de protection de données, ou encore les méthodes de recueil du consentement. De façon générale, l'enjeu sera de maintenir un équilibre entre la régulation de

[21] Conseil d'État, « *Etude annuelle 2014 du Conseil d'Etat - Le numérique et les droits fondamentaux* », *op. cit.*, p. 80.
[22] A. BRADFORD, « *The Brussels Effect* », vol. 107, 2012, Nw. U. L. REV., p. 1-68.
[23] « *Le Parlement européen a adopté le projet de réforme sur la protection des données* », europaforum.lu, 12 mars 2014, consulté le 7 novembre 2014, http://www.europaforum.public.lu/fr/actualites/2014/03/pe-protection-donnees/index.html.

l'existence des méthodes faisant appel au « *big data* » et la responsabilisation progressive des utilisateurs de données à caractère personnel. Ce dernier point est le corollaire de l'adaptation ou de l'assouplissement des exigences de consentement concernant le recueil de données. Le Conseil d'État souligne dans son rapport que de tels aménagements existent déjà, notamment pour le recueil de données à des fins statistiques, même si celles-ci ne sont pas strictement destinées à l'activité principale du collecteur. Il distingue ainsi ces données à caractère personnel mais à destination statistique des données destinées à cibler les individus, telles que les publicités comportementales.

Ainsi, parmi les propositions du Conseil d'État relevant du « *big data* », on trouve le renforcement de l'accès à l'information et le renforcement de la capacité à accorder un consentement éclairé. Ces propositions s'appuient par ailleurs sur la CNIL pour être menées à bien. Les instruments de régulation, s'ils ont besoin d'être affinés pour s'adapter à la mesure du « *big data* », peuvent globalement continuer de servir sous leur forme actuelle.

Un tel cadre de réglementation pourrait, par la suite, être accompagné d'une responsabilisation des acteurs du « *big data* ». Le renforcement de la protection accordée aux données que le nouveau règlement propose prend ainsi le parti de maintenir la forme du cadre actuel, fondé sur le consentement du citoyen, mais en allégeant les procédures en Union européenne par la centralisation du contrôle. On peut remarquer qu'un modèle similaire d'évaluation de risques, de partage d'information et de déclaration d'information ou d'utilisation existe, sur un sujet bien entendu très différent, sous la forme de la procédure REACH de contrôle des agents chimiques en Europe. La responsabilisation des acteurs semble, en effet, inévitable lors du traitement d'un nombre de données important. C'est finalement la conséquence de l'évolution permanente des technologies de « *big data* » et de « l'immobilité » relative du cadre juridique : il impose de faire confiance aux acteurs de cette évolution, à l'instar de l'arrêt *Google Spain c/ AEPD* du 13 mai 2014 de la CJUE.

CONCLUSION

C'est donc sur la confiance que l'on doit analyser le nouveau rôle joué par les utilisateurs de données. Comme nous l'avons souligné auparavant, l'utilisation attendue de données permet à l'utilisateur d'un service d'accorder son consentement. La question des symboles de confiance est ainsi une question importante : les protocoles SSL (*Secure sockets layer*) ou TLS (*Transport Layer Security*) se matérialisent sous la forme de cadenas qui assurent que la connexion est sûre, et notamment à l'abri d'espionnage ou « d'écoute ». De nombreux sites de paiement utilisent ce symbole pour assurer la confidentialité de la transmission d'informations bancaires, les cadenas sont devenus des symboles de sécurité et entretiennent ainsi la confiance de l'utilisateur. Le navigateur Mozilla Firefox propose pareillement une signalétique permettant d'identifier l'utilisation faite des données transmises[24]. En termes de navigation Internet, on pourrait ainsi imaginer une politique de signalétique qui informerait l'utilisateur des possibilités d'utilisation de ses données. Des données n'étant pas recueillies directement par Internet pourrait aussi en bénéficier, à travers l'informatisation d'un grand nombre de procédures quotidiennes, comme l'enregistrement pour une carte de fidélité. La

[24] Conseil d'État, « *Étude annuelle 2014 du Conseil d'État - Le numérique et les droits fondamentaux* », *op. cit.*, p. 181.

confiance de l'utilisateur doit être méritée pour permettre d'obtenir son consentement. Le cadre juridique de la protection des données, notamment face aux évolutions du « *big data* », doit donc être fondé à la fois sur un contrôle efficace comme le propose le cadre européen à venir, et sur la nécessaire responsabilisation des acteurs du « *big data* », dans la mesure où une simple logique réparatrice est trop lente et insatisfaisante face aux dangers d'un abus des données personnelles d'une personne. La liaison entre ces deux pôles serait le consentement et la confiance de l'utilisateur. La confiance permet de dépasser l'opposition entre « consentement éclairé » et utilisation indéfinie des données dans le cadre du « *big data* » dans la mesure où l'utilisateur a conscience de la réutilisation possible de ses propres données.

CLARISSE BERREBI

Les avocats et la transition numérique

CLARISSE BERREBI

Avocate associée, B&H Avocats

Présidente de la commission
Nouvelles technologies du Conseil
National des Barreaux

L'émergence des technologies de l'information et de la communication a profondément bouleversé l'environnement économique. Ces technologies ont permis l'émergence de nouveaux usages adoptés instantanément, et sans réserve, par une multitude d'individus. La révolution numérique crée un changement de paradigme de même ampleur que la révolution industrielle.

Les chiffres publiés par l'agence *We Are Social*, en octobre 2014, sont éclairants, quant à l'adoption du Web et des outils technologiques en un temps record : 41 % de la population mondiale utilise Internet, 83 % en France. 144 milliards d'emails sont échangés chaque jour. 90% des données numériques ont été créées ces deux dernières années.

Gains de temps, productivité, simplicité, ergonomie ont primé sur sécurité, maîtrise, secret, confidentialité. À tel point que les projets numériques sont toujours pensés d'abord en termes d'adoption de l'outil par les utilisateurs, ce qui constitue déjà un changement d'état d'esprit. C'est une déferlante qu'il est impossible de contrôler ou d'envisager de limiter.

Les avocats sont évidemment concernés au premier chef par ces questions qui sont au cœur de leur exercice professionnel et des relations dématérialisées qu'ils entretiennent entre eux, avec leurs clients et avec les juridictions.

I. LES ENJEUX

Les services grand public, comme Dropbox, Google, Amazon, Microsoft ou Yahoo, sont utilisés par la multitude des internautes y compris les avocats. Or, pour aucun de ces services les avocats ne sont en mesure de garantir la confidentialité des données qui transitent sur Internet. L'environnement dématérialisé génère de nouveaux risques pour la profession d'avocat qu'il convient, à défaut de les neutraliser, d'en assurer collectivement la maîtrise.

A. La garantie des droits fondamentaux à l'ère numérique

Les services grand public n'ont pas vocation à assurer pour une profession, fusse t-elle la profession d'avocat, la garantie d'un niveau de sécurité suffisant pour les données qui y transitent. Le secret professionnel des avocats n'est pas la priorité sur Internet. Il peut y avoir intrusion, et dans ce cas, elle s'avère aussi indolore qu'invisible et dramatiquement admise.

Le secret professionnel, lié au droit à la protection de la vie privée est le premier principe de la profession d'avocat. Il s'agit d'un droit et d'une garantie pour le client, ainsi que d'une obligation lourdement sanctionnée pour l'avocat. Sans la protection du secret de la confidence, les fonctions de défense et de conseil ne peuvent exister.

Dès lors, il appartient aux avocats de défendre le droit au secret sur ce vaste espace mondial qu'est le Web. Cette mission est d'envergure car à l'ère numérique, ère de la transparence et de la rapidité de transmission des flux, le droit au secret est menacé.

De façon générale, l'ère du Big Data, porteuse d'espoir pour une amélioration sensible de nos conditions de vie, porte en elle de lourdes menaces pour l'homme et ses droits fondamentaux. Le web conserve tout. Le passé demeure au présent et veut prédire le futur. Et le Big Data génère une querelle permanente entre le probable et le possible avec comme enjeu principal, le libre arbitre.

Les avocats, garant d'un état de droit, doivent être sensibilisés à ces risques.

B. Aider les avocats à investir massivement le Web en instaurant de la confiance pour les internautes

Pour autant, interdire l'utilisation par les avocats des outils grand public aurait été une double erreur. Tout d'abord, une telle interdiction aurait définitivement installé la déontologie de l'avocat dans la catégorie des vieilleries inadaptées à la réalité, à l'environnement économique et aux exigences d'un professionnel contemporain. Une telle décision empêchait l'accès de toute une profession à la modernité.

Ensuite, elle aurait éloigné les avocats scrupuleux d'une relation simple et directe avec leurs clients qui, chaque jour, utilisent les mails, les armoires électroniques, les transferts de fichiers volumineux, etc. Bref, les avocats se seraient fossilisés en tentant de protéger les données de leurs clients contre leur gré.

Au contraire, les avocats devaient accompagner ce mouvement et investir massivement le Web, territoire de droit, qui a besoin des avocats. C'est aussi un espace de création de valeur qui a entraîné une mutation de l'appréhension de l'espace et du temps[1].

La confidentialité y est indispensable, qu'il s'agisse par exemple de la confidence naturelle du client à son avocat, ou encore, dans le cadre d'une négociation entre avocats, de la possibilité pour le client de s'assurer que les termes de cette négociation ne puissent être divulgués.

[1] « *L'économie de l'immatériel est une économie systémique qui fonctionne en réseau et qui s'exonère des limites de temps et d'espace* ». Rapport de la commission sur l'économie de l'immatériel coprésidée par M. LÉVY et J.-P. JOUYET rendu en décembre 2007.

Récemment, un sondage institut IFOP – Ordre des avocats de Paris auprès de dirigeants de Petites et Moyennes Entreprises (PME) parisiennes a permis de confirmer que 84 % des chefs d'entreprises ont une bonne image des avocats et 87% ont confiance en eux.

La profession d'avocat dispose d'un important capital confiance, ce qui est précisément ce dont l'économie numérique a besoin. La déontologie de l'avocat se positionne alors sur le Web comme un avantage concurrentiel, une valeur historique de confiance et une puissante garantie de conscience de la valeur des droits, et en particulier des droits fondamentaux.

L'environnement numérique est particulièrement consommateur de confiance. Il se matérialise notamment par des questions simples : A qui je m'adresse ? Avec qui je contracte ? Qui est derrière l'ordinateur ? D'où viennent les flux ? Le Web a besoin d'intermédiaires capables d'identifier, d'authentifier, de sécuriser, de rassurer, de réaliser une transaction. Le Web a besoin de confiance et de sécurité.

Sur ce nouveau territoire à conquérir pour les avocats, il est impératif de doter les avocats d'une boite à outils les différenciant. Ces outils peuvent sans doute être acquis par les cabinets individuellement, mais cela nécessiterait alors d'importants coûts. Il était donc impératif que les instances professionnelles se mobilisent pour doter les avocats du minimum requis pour aborder l'environnement numérique et y devenir des interlocuteurs incontournables.

La réponse à ces exigences, a conduit la profession d'avocat à agir afin de permettre :

- l'authentification des avocats, la sécurisation des flux entre avocats, entre avocats et juridictions, entre avocats et clients ;

- un hébergement des données sur un Cloud maitrisé.

II. LES OUTILS INSTITUTIONNELS DE L'ENVIRONNEMENT NUMÉRIQUE

A ce jour, la profession d'avocat s'est dotée de trois outils majeurs pour aborder l'environnement numérique.

A. eBarreau

eBarreau est la plateforme permettant la communication par voie électronique entre avocats, et entre avocats et juridictions, dans le cadre de procédures en cours devant les Tribunaux de grande instance et les Cours d'appel, qu'il s'agisse des juridictions civiles, administratives et commerciales.

L'outil existe depuis 2007 et permet l'échange de messages électroniques dans un environnement très sécurisé. Précurseur sur la dématérialisation, cet outil a le mérite d'être utilisé par une immense majorité des avocats puisque 40 000 sur les 60 000 avocats inscrits à un barreau français utilisent quotidiennement eBarreau.

eBarreau subit actuellement de profondes mutations. En effet, il a été conçu pour échanger, mais la gestion par messages est très inconfortable puisqu'il s'agit d'une gestion chronologique

qui ne correspond pas à la réalité de la vie d'un dossier contentieux. Il est donc actuellement repensé, en collaboration étroite avec la Chancellerie, comme un outil collaboratif par dossier avec droits d'accès spécifiques selon les intervenants du dossier (avocat, greffe, magistrat, etc.).

Dans l'attente de la nouvelle plateforme eBarreau, l'outil a été modernisé. Une application eBarreau mobile permettant de maintenir un niveau de sécurité de connexion a été créée, pour permettre aux avocats de consulter les affaires à distance, recevoir les informations et consulter l'agenda des audiences.

Par ailleurs, eBarreau est la plateforme d'accès à Télérecours, outil de communication électronique devant les juridictions administratives, et iGreffe, outil de communication électronique devant les juridictions commerciales qui utilise la messagerie sécurisée d'eBarreau. Cet accès permet aux juridictions de s'assurer de l'identité de l'avocat connecté.

eBarreau est une plateforme web qui nécessite, en effet, une authentification forte pour y accéder. Cette authentification est permise par une clef token contenant un certificat d'authentification relié à un annuaire et permettant d'authentifier l'avocat et de confirmer son inscription à un barreau français en temps réel. Les flux sont ensuite chiffrés de l'avocat vers les greffes puis entre avocats.

B. eAA (l'acte d'avocat numérique natif)

L'acte d'avocat a été créé par la loi n° 2011-131 du 28 mars 2011 de modernisation des professions judiciaires ou juridiques et certaines professions réglementées, publiée au journal officiel du 29 mars 2011.

L'acte d'avocat a été inspiré de l'idée qu'il fallait élever la qualité de l'acte sous seing privé rédigé par un avocat. Il apporte des garanties aux contractants sur l'identité des parties et leur consentement éclairé. Il permet également de s'affranchir des mentions manuscrites. L'acte d'avocat est la manifestation de la confiance de l'État envers la profession d'avocat. Dans cette perspective, le Conseil national des barreaux a développé des formations à l'acte d'avocat et a élaboré des clauses types téléchargeables à partir du site internet www.actedavocats.fr.

La loi du 28 mars 2011, qui ajoute les articles 66-3-1 et s. à la loi n° 71-1130 du 31 décembre 1971[2], prévoit que la signature de l'avocat sur l'acte permet d'attester que les signataires auront reçu l'assistance juridique d'un avocat, qui les aura pleinement éclairés sur les conséquences juridiques de cet acte. S'agissant de son écriture et de sa signature, l'acte d'avocat est doté d'une force probante renforcée. A ce jour, il ne s'agit pas d'un acte que la loi impose.

La dématérialisation de l'acte d'avocat a été rendue possible par la combinaison des dispositions de la loi de 2011, et notamment l'absence de mentions manuscrites et la force

[2] Art. 66-3-1 : « *En contresignant un acte sous seing privé, l'avocat atteste avoir éclairé pleinement la ou les parties qu'il conseille sur les conséquences juridiques de cet acte* ».
Art. 66-3-2 : « *L'acte sous seing privé contresigné par les avocats de chacune des parties ou par l'avocat de toutes les parties fait pleine foi de l'écriture et de la signature de celles-ci tant à leur égard qu'à celui de leurs héritiers ou ayants cause. La procédure de faux prévue par le code de procédure civile lui est applicable* ».
Art. 66-3-3 : « *L'acte sous seing privé contresigné par avocat est, sauf disposition dérogeant expressément au présent article, dispensé de toute mention manuscrite exigée par la loi* ».

probante renforcée et, les dispositions des articles 1316-1 et suivants du Code civil qui, depuis 2000, octroient toute valeur juridique aux actes numériques natifs.

Il ne s'agit nullement d'opposer le papier au numérique. En revanche, le document qui fera foi, « l'original », n'est plus un document sous format papier. La dématérialisation de l'acte en facilitera sa conservation, limitera son altération et le risque de perte dans un environnement plus favorable à la mobilité. La notion « d'original » disparaît au profit d'une notion « d'authentique » qu'il sera toujours possible d'imprimer.

La version finale d'un acte électronique rédigée entre avocats et retenue par les parties sera déposée par l'avocat rédacteur sur un parapheur électronique. Ce parapheur électronique constitue le véritable enjeu du succès de l'acte d'avocat. Cet outil scellera la version ainsi déposée qui ne pourra subir aucune modification. Ce parapheur électronique doit être hébergé sur une plateforme gérée par le Conseil national des barreaux, tiers de confiance entre les avocats rédacteurs et contresignataires.

Le succès de la dématérialisation exige une gestion électronique des documents d'un bout à l'autre de leur élaboration afin de conserver leurs qualités et leur valeur probante qui seraient perdues si le document était imprimé puis numérisé.

S'agissant d'un acte sous seing privé, l'acte d'avocat dématérialisé devra d'abord recueillir la signature des parties dans les conditions de l'article 1316-4 du Code civil[3]. Un acte dématérialisé signé hors la présence des parties ne pourrait prospérer si une des parties signataires pouvait s'inquiéter du sérieux de l'identification de son cocontractant.

L'avocat ajoute à sa mission traditionnelle de vérification de l'identité de son client, le rôle d'autorité d'enregistrement en demandant la délivrance d'un certificat de signature électronique à l'instar des établissements bancaires pour les achats en ligne. Il s'agit d'un certificat éphémère délivré par une autorité de certification sur demande de l'avocat.

Dès lors que les parties auront signé l'acte, l'avocat ou les avocats pourront alors le contresigner grâce à leur clef token d'authentification forte, délivrée pour l'utilisation de e-Barreau.

---

[3] Article 1316-1 du Code civil, créé par Loi n°2000-230 du 13 mars 2000 : « *l'écrit sous forme électronique est admis en preuve au même titre que l'écrit sur support papier, sous réserve que puisse être dûment identifiée la personne dont il émane et qu'il soit établi et conservé dans des conditions de nature à en garantir l'intégrité* ».
Article 1316-3 du Code civil : « *L'écrit sur support électronique a la même force probante que l'écrit sur support papier* ».
Article 1316-4 du Code civil « *La signature nécessaire à la perfection d'un acte juridique identifie celui qui l'appose. Elle manifeste le consentement des parties aux obligations qui découlent de cet acte. Quand elle est apposée par un officier public, elle confère l'authenticité à l'acte.*
Lorsqu'elle est électronique, elle consiste en l'usage d'un procédé fiable d'identification garantissant son lien avec l'acte auquel elle s'attache. La fiabilité de ce procédé est présumée, jusqu'à preuve contraire, lorsque la signature électronique est créée, l'identité du signataire assurée et l'intégrité de l'acte garantie, dans des conditions fixées par décret en Conseil d'Etat ».
Décret n°2001-272 du 30 mars 2001 pris pour l'application de l'article 1316-4 du Code civil et relatif à la signature électronique, Article 2 : « *La fiabilité d'un procédé de signature électronique est présumée jusqu'à preuve contraire lorsque ce procédé met en œuvre une signature électronique sécurisée, établie grâce à un dispositif sécurisé de création de signature électronique et que la vérification de cette signature repose sur l'utilisation d'un certificat électronique qualifié* ».

Cette technologie permettra de signer un acte à distance, de façon asynchrone et, sans présence physique au moment de la signature ; un face à face n'étant indispensable qu'au moment de la délivrance du certificat et de la réception des pièces le justifiant.

L'acte d'avocat dématérialisé pourra être imprimé, téléchargé et conservé par le client sur ses propres serveurs. Il devra aussi pouvoir être retrouvé par l'avocat chez l'hébergeur de confiance sur les serveurs duquel il aura été déposé. Son intégrité sera assurée pendant une période de 5 à 75 ans.

Cette plateforme permettra en outre de numériser des actes signés sous format papier et de les signer électroniquement afin de leur adosser une date certifiée et de procéder à leur archivage long terme.

C. Cloud privé des avocats

Le Cloud privé des avocats a été imaginé par le Conseil National des Barreaux pour permettre à la profession d'avocat et à chacun de ses membres de disposer d'une solution fiable, souple, intelligente et ergonomique qui permette de s'assurer de :

- la souveraineté des données (mails, agenda, contacts, drive, etc.) hébergées sur Internet ;

- niveau de chiffrement et des droits d'accès ;

- la certitude d'échanges sécurisés entre avocats ;

- une possibilité de chiffrage simple et ne nécessitant pas de compétence technique des échanges entre l'avocat et le client.

L'avocat, dès sa prestation de serment, et quelque soit le cabinet dans lequel il évolue, doit individuellement disposer des outils professionnels et différenciants lui permettant de travailler grâce, et avec, Internet dans un environnement garantissant le respect de ses obligations déontologiques.

L'avocat doit pouvoir disposer d'une adresse e-mail équivalente à une toque virtuelle, et d'un espace de travail virtuel lui garantissant le respect des principes essentiels[4].

L'objectif est d'éviter que l'avocat n'envisage spontanément l'ouverture d'un compte Gmail – par exemple – ou l'utilisation de Dropbox – par exemple – comme serveur de fichiers ou toutes ces messageries ou serveurs Cloud grand public qui ont d'importantes lacunes en termes de confidentialité et de sécurité – profilage, vente de données anonymisées, publicité ciblée, stockage en clair, traçage des données de connexion, Patriot Act.

[4] Ces principes sont définis par les articles 1 à 5 du décret du 12 juillet 2005 relatif aux règles de déontologie de la profession d'avocat (http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000633327) ainsi que par l'article 1 du Règlement Intérieur national de la profession d'avocat (RIN) (http://cnb.avocat.fr/Reglement-Interieur-National-de-la-profession-d-avocat-RIN_a281.html#1).

CONCLUSION

La nouvelle ère qui s'est amorcée a profondément modifié les usages des citoyens. Ces changements vont sans doute impliquer des modifications profondes de nos usages, en tant que professionnels responsables, chargés d'une mission spécifique d'accès au droit et de défense des intérêts de nos clients.

Les avocats sont bousculés par le marché qui permet l'émergence d'interlocuteurs non réglementés qui rendent des services de nature juridique ou quelque fois donnent des conseils.

Dotés des outils numériques indispensables, les avocats s'adapteront sans doute à cet environnement, notamment s'ils s'attachent à préserver leur différence et leurs obligations déontologiques en tant que contreparties des droits fondamentaux de leurs clients.

Il est vraisemblable que les avocats ne sont plus pourvoyeurs d'information à l'ère numérique, et devront adapter leur façon d'appréhender l'information, de traiter leurs dossiers et de communiquer avec les internautes.

Il n'y a pas de doute qu'ils le feront et que le World Wide Web deviendra un véritable espace de droits, d'échanges et de vie au sein duquel les droits fondamentaux des citoyens-internautes seront respectés avec et grâce aux avocats qui l'auront massivement investi.

ÉCOLE DE DROIT

Compte-rendu de la conférence « Barreau 2.0 : Update & Upgrade ! »

Par Marin Denizet et François Weidler-Bauchez, membres du Comité de rédaction de la Revue des juristes de Sciences Po

RÉSUMÉ

L'Incubateur du Barreau de Paris, créé à l'initiative de ***Frédéric Pelouze*** *(lanceur en 2013 de la première société française de financement de contentieux : Alter Litigation Ltd.),* ***Lise Damelet*** *(avocat collaborateur, Orrick Rambaud Martel),* ***Adrien Perrot*** *(associé, cabinet Deprez Perrot) et* ***Alexandra Uhel*** *(avocat collaborateur, Linklaters), est un signe de plus de la nécessaire adaptation des professions juridiques à l'ère du XXI*ème *siècle et des progrès technologiques.*

Le lancement de l'Incubateur, premier incubateur européen dédié aux prestations de services juridiques, en ce 9 octobre 2014, a donc été l'occasion pour les intervenants d'exposer leurs points de vue autour des grandes questions et enjeux, et des futurs bouleversements auxquels va se trouver confronté le monde du droit.

La première table ronde a été l'occasion de rappeler l'apparition d'un écosystème de start-ups juridiques à travers le monde, y compris en France, à l'image de ce qui est en train de se produire aux Etats-Unis ; la seconde a abordé l'épineux problème du mode de financement externe des cabinets d'avocats ; la troisième s'est attachée à relever l'émergence de nouveaux modes de formation des juristes français.

A l'occasion du lancement de l'Incubateur du Barreau de Paris, premier incubateur européen dédié aux prestations de services juridiques, s'est tenue le 9 octobre 2014 la conférence « Barreau 2.0 : Update & Upgrade ! ».

La première table ronde de la conférence portait sur les défis posés par l'intelligence artificielle appliquée aux prestations de services juridiques. Partant du constat que le progrès technologique était sans précédent, et que d'ici à la prochaine décennie, les ordinateurs disposeront d'un niveau d'intelligence équivalent à celui du cerveau humain, ces ordinateurs seraient bientôt capables de remplacer les avocats dans la réalisation d'un certain nombre de taches juridiques. Par ailleurs, ces bouleversements atteindraient le « périmètre du droit », jusqu'alors protégé des innovations, les juristes étant décrits comme rétifs au risque et au changement.

L'apparition d'une offre pléthorique de sites internet juridiques outre-Atlantique appelle déjà à une redéfinition du rôle de l'avocat traditionnel. *Legalstart.fr* propose des prestations juridiques dématérialisées et permet d'élargir l'audience du droit au plus grand nombre. Pierre Aïdan, co-fondateur de *Legalstart.fr*, explique qu'aux Etats-Unis, l'American Bar Association vient de conclure un accord avec le numéro deux du secteur afin de pallier les difficultés d'accès aux services juridiques. Pour illustration, en France, plus de 50% des PME

n'ont jamais recours à un avocat alors qu'au cours des douze derniers mois, 40% d'entre elles ont connu un problème juridique majeur.

Si les avocats veulent continuer à répondre à la totalité des besoins juridiques sans être marginalisés, ils doivent réinventer leur offre. Dans le cas contraire, ils ne seront plus que des sous-traitants de ce type de sociétés qui systématisent les opérations juridiques simples pour confier les cas les plus complexes, et donc les plus rares, à une minorité d'avocats.

Les intervenants de la deuxième table ronde se sont penchés sur les modes de financement externes des cabinets d'avocats. En effet, les cabinets français sont confrontés à une concurrence croissante de la part des cabinets anglo-saxons et des professions connexes, mais également à des chocs technologiques exacerbant la pression concurrentielle. Lionel Scotto, fondateur du cabinet éponyme, tire la sonnette d'alarme quant à la compétitivité de son cabinet sur le marché : « *Je ne peux plus lutter à armes égales, le talent ne fait pas tout et il devient impossible de concurrencer les cabinets internationaux* ». Dans un premier temps, l'idée est de recourir, non à la forme actionnariale mais partenariale – avec inter-professionnalité – afin d'abaisser les coûts des cabinets en opérant des synergies.

La discussion s'est alors cristallisée sur le maintien de l'indépendance de l'avocat et du secret professionnel dans la perspective d'une ouverture du capital à ces investisseurs connexes à la profession et non soumis à la déontologie de l'avocat. A ce propos, Alexandre Désy, avocat au barreau du Québec, a tenu à rappeler que le capital des cabinets d'avocats québécois est ouvert jusqu'à 49% à des investisseurs extérieurs à la région, et ce depuis dix ans, sans que cela ne pose de problème.

Un ancien membre du Conseil de l'Ordre, Christophe Thévenet, a ensuite mis en exergue le fossé existant entre une minorité de grands cabinets d'affaires et une majorité de petits cabinets qui exerce dans la matière judiciaire. Selon lui, « *la grande majorité des avocats ne se sent pas concernée par ce débat sur le financement* », le vote négatif du CNB sur l'ouverture du capital des cabinets en est l'illustration.

Tout en accordant une place à « *un modèle de financement qui intéresse aussi les petits cabinets qui font du judiciaire* », il devient urgent de répondre à ce besoin de financement.

Autour de la troisième table ronde, Jean-Louis Scaringella, actuel directeur de l'EFB, anciennement à la tête d'HEC et de l'ESCP Europe, s'est attaché à rappeler la vocation de l'EFB. Celle-ci n'est pas d'enseigner le droit mais bien de se servir du droit : il s'agit, en ses termes, d'une « *école d'apprentis* ».

L'Université, représentée par l'intermédiaire du professeur Pierre-Yves Gautier, a également tenu à défendre son modèle et a soutenu que les élèves étaient soumis à des cas pratiques – qui n'en restent pas moins théoriques – dès la formation initiale, y compris lors du 1er cycle.

Jérémy Perelman, directeur de la Clinique de l'Ecole de droit, rappelle que l'un des buts poursuivis par la Clinique, et plus généralement l'Ecole de droit, est « *de mieux appréhender le droit dans la vraie vie* ». Les projets au sein des cliniques, et le développement exponentiel que celles-ci connaissent outre-Atlantique, en témoignent.

Michael J. Borden, professeur associé à l'université Cleveland-Marshall aux Etats-Unis, a souligné que cela faisait maintenant de nombreuses années que l'apprentissage du droit de Common Law s'attachait bien plus aux faits qu'au droit en tant que tel, évolutif par nature.

La mutation des formations initiales de droit en France est donc lancée, y compris sous l'impulsion d'organismes privés comme l'Ecole des Hautes Etudes Appliquées du Droit (HEAD).

Compte-rendu du Google Advisory Council Meeting (tenu à Paris le 25 septembre 2014)

Par Carolin Stenz, membre du Comité de rédaction de la Revue des juristes de Sciences Po

A travers l'arrêt *Google Spain SL*, la CJUE semble avoir ramené la question de la gouvernance de l'Internet au XXI^{ème} siècle : qu'est-ce que un moteur de recherche et qu'est-ce que le droit à la vie privée ? Suite à cette décision, le moteur de recherche se voit conférer la qualité d'« *éditeur* » et Google est désormais responsable de ses résultats de recherche s'il s'agit de l'identité d'une personne. Lors de l'*advisory council meeting* à Paris, des experts venant de différents horizons professionnels ont donné leurs avis sur comment interpréter la décision de la CJUE et comment assurer cette tâche.

La décision de la Cour de Justice de l'Union Européenne, du 13 mai 2014, sur le droit au déréférencement – communément appelé le droit à l'oubli – relève de ces décisions fondatrices qui, par la solution qu'elles apportent en particulier à un litige, ouvrent simultanément grande une porte vers de nouvelles questions juridiques.

Un an plus tôt, en référence au droit à la liberté d'expression, la Cour Européenne des Droits de l'Homme avait rejeté une demande de suppression d'un article de presse supposé nuire à la réputation de deux avocats polonais susceptibles d'avoir assisté des hommes politiques pour des transactions commerciales douteuses.[1]

Dans le différend C131/12 *Google Spain SL, Google Inc. contre Agencia Española de Protección de Datos (AEPD), Mario Costeja González*, un entrepreneur espagnol avait demandé la suppression des liens, dans les résultats de la recherche Google, vers deux articles relatant une mise aux enchères d'une maison, à la suite du non-paiement de ses cotisations sociales. A cet effet, la CJUE a privilégié le droit à la vie privée : désormais les liens doivent être retirés de la liste des résultats de recherche « *lorsque ces données ne sont plus nécessaires au regard des finalités pour lesquelles elles ont été collectées ou traitées. Tel est notamment le cas lorsqu'elles apparaissent inadéquates, qu'elles ne sont pas ou plus pertinentes ou sont excessives au regard de ces finalités et du temps qui s'est écoulé* »[2].

Par sa décision, la CJUE attribue au moteur de recherche la qualité d'éditeur, et en tant que tel, une responsabilité sur le traitement des données à caractère personnel ; ce qui entre en conflit avec l'image de « *world library card index* » que Google essaie de défendre. En réponse à la décision de la CJUE, Google a mis en ligne un formulaire de demandes de déréférencement à travers lequel plus de 135 000 demandes relatives à 475 000 URL ont été déposées. L'intérêt pour Google, dans les réunions dans différentes capitales européennes, de ce comité consultatif de 9 experts – dont 7 présents à Paris – est de déterminer, à l'horizon du début de

[1] CEDH, arrêt *Węgrzynowski et Smolczewski/Pologne*, requête n° 33846/07, 16 juillet 2013.
[2] CJUE, arrêt *Google Spain* et *Google/Agencia Española de Protección de Datos (AEPD) et Mario Costeja González*, requête n° C-131/12, n° 93, 13 mai 2014.

l'année 2015, comment caractériser précisément les critères susmentionnés : informations inappropriées, sans pertinence, excessives ou obsolètes, afin de satisfaire à l'obligation de référencement. Parmi les questions sur lesquelles le comité se penche figurent celles concernant le traitement des « *cas complexes* » : personnes de la vie publique, personnes condamnées ou non pour des crimes, question du déréférencement temporaire ou permanent, etc.[3].

Le premier des deux volets de la réunion était consacré à des experts venant d'horizons divers.

Le psychologue, psychiatre et psychanalyste Serge Tisseron, directeur de recherche à l'Université Paris VII Denis Diderot, spécialisé dans le domaine des secrets de familles et des rapports aux nouvelles technologies, plaide contre tout droit de déréférencement et de retrait des informations que toute personne aurait publié sur internet d'elle-même. Il alerte contre un « droit à l'oubli » ou « droit au repentir », non seulement en raison de la responsabilité, mais aussi et avant tout d'un point de vue mémoriel, en attribuant à l'Internet ladite qualité de mémoire.

Benoît Louvet, représentant de la LICRA, la Ligue internationale contre le racisme et l'antisémitisme, se prononce lui en faveur d'un « droit à l'oubli » total pour les victimes d'agression et de violence racistes, mais demande une prudence particulière pour le déréférencement des auteurs de telles agressions et des thèses négationnistes. Son intervention met en évidence la difficulté de juger et d'établir un critère intersubjectif ; à savoir si une fois subie la peine infligée, ou en cas de non condamnation, il devrait être possible de demander le déréférencement, ou si cette information devrait rester accessible. Par rapport à ce deuxième aspect, M Louvet se montre favorable – sous certaines réserves de prudence – au critère de la vérité juridique.

Dans son intervention, Emmanuel Parody, représentant des éditeurs et secrétaire général de GESTE, le Groupement des éditeurs de services en ligne, quant à lui, remet en cause la décision de la CJUE conférant à Google la qualité d'éditeur. Selon Emmanuel Parody, l'abandon du concept de la neutralité du moteur de recherche mettrait en danger son autonomie, et ouvrirait la voie au risque d'instrumentalisation. Au lieu d'un simple déréférencement effectué par Google, Parody se prononce en faveur d'un processus d'échange et de conseil entre le moteur de recherche et l'éditeur de l'information, qui serait souvent mieux placé pour juger de l'obsolescence d'un contenu ou de son aspect inapproprié.

Bertrand Girin, co-fondateur de *www.forget.me*, une plate-forme intermédiaire proposant de l'aide à la rédaction des demandes de suppression des liens pour Google et Bing, partage ses expériences et parle des motivations concrètes des demandeurs de déréférencement. Il rappelle que la plupart des cas gérés via *forget.me* sont des cas, non pas complexes, mais simples, relevant strictement de la vie privée sans intérêt public – injures, dévoilements de la vie familiale de personnes hors sphère de la vie publique, ou autres. Le plus dérangeant pour

[3] CJUE, 13 mai 2014, n° 81 : « *Si, certes, les droits de la personne concernée protégés par ces articles prévalent également, en règle générale, sur ledit intérêt des internautes, cet équilibre peut toutefois dépendre, dans des cas particuliers, de la nature de l'information en question et de sa sensibilité pour la vie privée de la personne concernée ainsi que de l'intérêt du public à disposer de cette information, lequel peut varier, notamment, en fonction du rôle joué par cette personne dans la vie publique* ».

ces gens, selon M. Girin, est que cette information puisse apparaître en première page « *comme si elle était gravée sur leur front* ».

Le deuxième volet de cette réunion était consacré aux experts juridiques.

Marguerite Arnaud, auteur d'un mémoire portant sur le droit à l'oubli, et aujourd'hui avocate chez Lawways Avocats, aborde la décision de la CJUE quant au droit au déréférencement pour les personnes de notoriété publique. Elle observe que la Cour est restée cohérente à sa propre jurisprudence, et à celle de la CEDH, dans la mesure où elle n'a pas refusé tout droit au déréférencement aux personnes publiques, tout en prenant en compte que leur rôle particulier dans la vie publique exige une précaution particulière par rapport à la décision de déréférencer.

Céline Castets-Renard, Professeur de droit privé à l'université Toulouse I Capitole, et spécialiste du droit de l'Internet, à son tour, rappelle que la décision porte en elle le risque que le moteur de recherche se mette à la place du juge. Contrairement à cette idée, et conformément à la décision du Conseil Constitutionnel du 10 juin 2004, elle avance le principe de jurisprudence française de « manifeste » pour décider sur le déréférencement, et conseille, en cas de doute, de s'abstenir de déréférencer. Les décisions sur les cas complexes et la mise en balance des droits fondamentaux (liberté d'expression et protection de la vie privée) appartiendraient au juge et non pas au moteur de recherche.

Dans son intervention, Bertrand de la Chapelle, directeur du projet « Internet&Jurisdiction », plate-forme créé dans le but de faciliter l'échange entre les différentes parties prenantes sur la réglementation de l'Internet, revient sur des aspects concrets dans ce processus de déréférencement. Il insiste sur l'importance d notification aux éditeurs du déréférencement d'une information, et se prononce en faveur de la mise en place d'une structure décisionnelle à l'extérieur du moteur de recherche, afin de balancer les intérêts des parties impliquées. Surtout, pour les cas sensibles où une personne, ayant obtenu un déréférencement de certains contenus, se présenterait pour un mandat public, alors, par une collaboration étroite entre moteur de recherche et éditeur, M. de La Chapelle entrevoit la possibilité d'une plus grande efficacité, en écartant le risque de nouveau déréférencement.

Laurent Cytermann, Rapporteur général adjoint au Conseil d'État 2014 du rapport des droits fondamentaux dans le domaine du numérique, rejoint les autres intervenants sur l'importance d'inclure les éditeurs même à un degré élevé : non seulement il serait souhaitable de les informer *a posteriori*, mais de les impliquer activement pour qu'il y ait une troisième partie, et pour que la décision de déréférencement ne soit pas prise en tête-à-tête entre le moteur de recherche et l'individu. Il reprend l'idée, également avancée par Bertrand de La Chapelle, de globaliser les demandes de déréférencement pour tous les moteurs de recherche par reconnaissance mutuelle, afin de faciliter l'exercice de ce droit. En outre, il revient, lors son intervention, sur le problème de la territorialité et la question en suspens de savoir si le droit au déréférencement pourrait également être étendu sur les versions non-européennes des moteurs de recherche, pour un citoyen de l'Union Européenne, ce qui, à l'heure actuelle, reste contesté.

Actualités de l'École de droit

ECOLE DE DROIT

Le 30 août 2014, l'Ecole de Droit de Sciences Po comptait 480 étudiants. L'École a eu le plaisir d'accueillir 222 nouveaux élèves. 185 d'entre eux ont intégré le master Droit Economique et 37 ont rejoint le Master Carrières Juridiques et Judiciaires. Actuellement, 133 étudiants continuent leur formation en deuxième année de Droit Economique, 25 poursuivent en Carrières Juridiques et Judiciaires et 100 sont en césure ou bénéficient d'un parcours aménagé.

EVÈNEMENTS

22 septembre 2014 : Conférence « Responsabilité des cabinets d'avocats : Etats des lieux et perspectives »

En ce début septembre, la Clinique de l'École de Droit a organisé une conférence sur la « ***Responsabilité des cabinets d'avocats : Etats des lieux et perspectives*** », interrogeant l'application des principes inspirés de la Responsabilité Sociale et Environnementale (RSE) au sein des cabinets d'avocats. Les initiateurs de l'étude de la Clinique relative au sujet sont intervenus à l'invitation de **Christophe Jamin**, directeur de l'Ecole de Droit et **Pierre-Olivier Sur,** bâtonnier du Barreau de Paris. Ainsi, **Paul Lignières,** *managing partner* de Linklaters, **Christopher Baker**, avocat et maître de conférence à Sciences Po, **Jeremy Perelman**, *assistant professor* et responsable de la Clinique de l'Ecole de Droit de Sciences Po ainsi que **Marie Bouchard,** élève avocat, et **Alexis Giroulet**, ancien étudiant de l'École de Droit, ont pu présenter le résultat de leur étude.

29 septembre 2014 : Colloque « Comment construire des politiques fiscales internationales durables ? »

L'invitation de l'Ecole de droit à la Maison de la Chimie a eu pour but de réfléchir autour de la question de « ***Comment construire des politiques fiscales internationales durables ?*** ». Dans un contexte de crise où les questions de fiscalité, tant nationales qu'internationales, sont devenues centrales pour les acteurs économiques, l'invitation de l'Ecole de Droit au colloque a permis aux praticiens du secteur public ou privé, aux étudiants, aux universitaires et autres participants, d'acquérir une vision globale des principes et enjeux de base des politiques fiscales et d'échanger au sujet de la question de la construction de politiques fiscales internationales durables.

16 octobre 2014 : Conférence « Performance and corporate integrity: a new paradigm for companies in the XXIst century »

Bein Heinemen, vice-président et directeur juridique de General Electric, professeur à Harvard et Yale, auteur de « *High Performance With High Integrity* » a eu l'occasion d'apporter son expertise personnelle relative à la prise en considération des valeurs éthiques dans le management de la performance. L'essentiel de la présentation s'est focalisée sur son

expérience chez General Electric et a ainsi donné aux étudiants une vision concrète des problématiques de gouvernance actuelles.

20 et 21 octobre 2014 : Journées d'étude « La prévention des récidives : Evaluation, suivis, partenariats »

En partenariat avec la direction de l'administration pénitentiaire, avec le soutien de la mission de recherche Droit et Justice, l'Ecole de Droit a dédié les journées des 20 et 21 Octobre à ***« La prévention des récidives : Evaluation, suivis, partenariats »***. Ces journées d'études internationales étaient placées sous le haut patronage de Madame **Christiane Taubira**, Garde des Sceaux, ministre de la Justice. Des conférences et des tables rondes ont réuni pour les étudiants de Sciences Po, des praticiens, des universitaires et des chercheurs internationaux concernés par les mutations de l'institution pénitentiaire.

3 décembre 2014 : Conférence annuelle de l'AJSP « Le droit des entreprises en difficulté permet-il de concilier les intérêts des différents acteurs en présence ? Réponse par l'exemple »

La conférence traditionnelle de l'AJSP en partenariat avec CMS Bureau Francis Lefebvre fut suivie de la remise des pulls de l´École de Droit. Le débat a porté sur le traitement des difficultés des entreprises au lendemain d'une réforme législative visant à remédier à l'inquiétant taux de défaillance des entreprises. **Sergio Trevino**, CEO du Groupe Brandt, a apporté son expérience précieuse sur la question au travers de l'exemple de FagorBrandt. **Xavier Gelot**, Rapporteur au Comité Interministériel de Restructuration industrielle de la direction générale du Trésor, **M^e^ Gaël Couturier**, administrateur judiciaire associé, **M^e^ Alain Herrman**, associé du cabinet CMS Bureau Francis Lefèbvre ont mis en lumières les différents enjeux du traitement juridique des entreprises en difficulté. **M^e^ Alexandre Bastos**, responsable de l'activité des Entreprises en difficulté du cabinet CMS Bureau Francis Lefèbvre, a modéré le débat.

17 février : Conférence « Les objets connectés : une perspective juridique »

La conférence organisée en partenariat avec le cabinet Hogan Lovells s'est focalisée sur un sujet transversal entre le droit de la propriété intellectuelle et les nouvelles technologies. **Christine Gateau**, **Christelle Coslin** et **Stanislas Roux-Vaillard**, trois avocats spécialistes du droit des NTIC au sein du cabinet Hogan Lovells, ont débattu sur les bénéfices et les enjeux du développement massif des objets connectés.

LES PETITS-DÉJEUNERS DE L'AJSP

29 octobre 2014 : Fusions-acquisitions

Le premier petit déjeuner de l'année fut organisé au sein des bureaux parisiens de Gide Loyrette Nouel en présence de **M^e^ Guillaume Rougier-Brierre**, avocat spécialisé en fusions-acquisitions et droit des sociétés. Celui-ci a pu transmettre aux étudiants son expérience et ses conseils afin de les aider à construire leur projet professionnel.

4 novembre 2014 : Recherche

Le petit-déjeuner « Recherche » a accueilli le Professeur **Guillaume Tusseau**, ainsi que deux doctorants de l'Ecole de Droit de Sciences Po, **Aurélien Bouayad** et **Bamdad Shams**. Cette matinée a permis aux étudiants intéressés par le droit public et la recherche d'affiner leurs projets d'étude au sein de Sciences Po.

18 novembre 2014 : Droit social

Ce petit-déjeuner a eu lieu les locaux du cabinet CMS Francis Lefebvre. **Me Ludovique Clavreul** a éclairé les participants sur la pratique quotidienne de son métier et **Mesdames Anne de Wilde et Emilie Gaunand** ont fourni de précieuses informations relatives au recrutement.

20 novembre : Droit pénal

Les étudiants intéressés par le droit pénal se sont réuni autour de **Me Grégoire Etrillard**, avocat pénaliste.

26 novembre : Corporate

Petit-déjeuner au sein du département Corporate du cabinet Dechert LLP. **Me Guillaume Briant** et **Me François Hellot** ont accueilli les étudiants et ont partagé leurs expériences et leurs visions sur le marché du Corporate

28 janvier : Cabinet Herbert Smith Freehills

Pour le premier petit-déjeuner AJSP de l´année 2015, l'AJSP a donné rendez-vous aux intéressés au cabinet Herbert Smith Freehills. Environ une quinzaine d´étudiants ont pu profiter des parcours et expériences de **Me Eric Fiszelson** (département M&A, Project Finance, droit bancaire), **Me Leïla Hubeaut** (département M&A, Énergie et infrastructures), et **Me Clément Dupoirier** (département contentieux).

6 février : Fusions-acquisitions, restructuration, concurrence, régulation

L'AJSP a eu la chance d'être invitée par les associés du cabinet BDGS, spécialisés dans les opérations de fusions-acquisitions, restructurations et les questions de concurrence et de régulation. Les membres fondateurs de BDGS, créé en avril 2013, sont tous issus du cabinet Gide Loyrette Nouel. Les élèves ont été accueillis par les associés fondateurs **Maîtres Djehane**, **Gosset-Grainville** et **Skovron** et par **Maîtres Loy** et **Devouge**.

Mardi 10 février : Petit-déjeuner avec Felicia Henderson

Avocate américaine, **Felicia Henderson** a exercé à New York et à Paris en tant que « *corporate lawyer* », avant de se tourner vers l'enseignement et le consulting indépendant auprès de dirigeants. Après avoir partagé son parcours professionnel et abordé les différences culturelles entre avocats new-yorkais et parisiens, Mme Henderson a pu donner ses précieux conseils aux

étudiants.

Jeudi 12 février : Propriété intellectuelle

SciencesPo a convié les étudiants intéressés à un petit-déjeuner sur la propriété intellectuelle. Les trois intervenants aux parcours variés ont pu renseigner les participants sur les débouchés possibles dans ce domaine. **Séverine Dusollier**, professeur au sein de la spécialité Droit de l'innovation du master Droit économique, **Denis Monégier du Sorbier**, *Managing Partner* du cabinet d'avocats **Hoyng Monégier**, et **Vincent Ruzek**, juriste PI chez L'Oreal ont contribué à la réussite de cette matinée.

Moots

Pour la quatrième année consécutive, l'Ecole de Droit a participé à la *Competencia de Arbitraje Comercial Internacional* organisée par l'Universidad del Rosario (Colombie) et l'Universidad de Buenos Aires (Argentine) à Lima. Réunissant 47 équipes, la compétition demandait à traiter de la demande de reconnaissance et de l'exécution d'une sentence arbitrale étrangère. L'équipe de l'Ecole de Droit, soutenue par le Professeur **Diego P. Fernandez Arroyo**, coachée par **Ruxandra Esanu** et financée par le cabinet Dechert LLP, s'est distinguée parmi les meilleures de la compétition. **Paloma Garcia Guerra** est arrivée sixième de la compétition des meilleurs orateurs, **Filipe Antunes Madeira da Silva** a obtenu une mention spéciale pour avoir obtenue une note exceptionnelle lors d'une audience.

Appel à contributions

Numéro 11 : la violence et le droit

Le constat n'a pas grand chose de révolutionnaire : droit et violence sont indissociables. Loin de lui fournir uniquement un objet de lutte, elle en constitue aussi – de manière moins immédiatement perceptible – tant un moyen qu'une conséquence. En d'autres termes, la violence n'est pas étrangère au droit dans ses modalités, mais opère directement en son sein – par et pour lui. Il échoue ainsi irrémédiablement dans son entreprise répressive, du fait de sa structure et ses objectifs initiaux.

Cette dichotomie dessine deux sources contraires de corrélation : l'assimilation de la violence par le droit, d'une part, et le mouvement plus répulsif de mise à distance, de protection, d'autre part. Le droit est en effet la condition nécessaire à la mise en place des principaux cadres de légitimation de l'exercice de la violence étatique – comme de la résistance à ses abus – et, plus largement, de la violence sociale et économique.

Dans une perspective transversale, le comité de rédaction de la Revue des Juristes de Sciences Po a décidé d'orienter le dossier thématique de son prochain numéro sur les rapports complexes et parfois contradictoires entre droit et violence. Ces enjeux englobent non seulement le droit pénal, bien entendu, mais aussi le domaine civil, où la Haute juridiction a considéré, plus influencée par les évolutions de la société que jamais, qu'une violence était aussi économique. Les régulateurs, plus puissants qu'hier, cherchent à exercer leurs prérogatives en usant de moyens coercitifs de plus en plus violents.

Ainsi, les thèmes suivants pourront notamment faire l'objet de contributions :

- Violence et droit pénal
    - Le droit pénal comme moyen indispensable et légitime à la régulation de la violence
    - L'application de la violence pénale au droit des affaires et les évolutions qui en procèdent
    - Le droit pénal : violence contre violence ?
    - Éthique, domaine pénal et violence
    - Procédure et polymorphie de la violence
    - Prise en compte juridique des violences psychologiques
- Droit civil et violence économique

- Droit commercial et violence inhérente à la rupture brutale des relations

- Violence et droit international

    - La violence transnationale du conflit de lois

    - Le droit de la guerre : légitimation de la barbarie ?

- Les marges de manœuvres procédurales des Autorités Administratives Indépendantes (AAI) et leur force coercitive

- Violence médiatique des affaires judiciaires (facteur de dissuasion supplémentaire à l'infraction ?)

Cette liste non exhaustive ne présente que quelques pistes de recherche. N'hésitez donc pas à nous proposer des thèmes de contribution différents, toutes les idées étant les bienvenues. Si vous souhaitez participer à ce numéro, vous pouvez nous contacter à l'adresse suivante :

revue.ajsp@gmail.com

Les propositions de contributions doivent être envoyées avant le 30 avril 2015.

Les articles dans leur version finale devront être envoyés avant le 30 juin 2015.

Nous nous tenons à votre disposition pour toute information complémentaire et attendons avec impatience vos contributions.

Le Comité de rédaction de la Revue des Juristes de Sciences Po

La Revue des Juristes de Sciences Po

Revue éditée par l'Association des élèves et diplômés Juristes de Sciences Po (AJSP)
ISSN 2111-4293

27, rue Saint-Guillaume - Paris
Email : revue.ajsp@gmail.com
Site : http://AJSP.FR

Supervision Scientifique du Dossier thématique :
Jean-Baptiste Soufron

Rédactrice en chef :
Gwennhaëlle Barral

Rédacteur en chef adjoint et responsable de la publication :
Victor Charpiat

Citation de la Revue :
RDJScpo, nº 10, Hiver 2015, p. X