Que deviennent les données numériques des défunts ?

La notion de « mort numérique » renvoie à la question du devenir des données numériques des défunts. La loi et la jurisprudence sont venues préciser les droits des héritiers ou des proches.

Les droits des héritiers ou des proches sur les données numériques des défunts

Qu'en est-il de l'accès aux **profils sur les réseaux sociaux** et aux **comptes de messagerie** d'une personne décédée ?

L'ouverture d'un compte de messagerie ou d'un compte sur un réseau social confère à son titulaire des droits personnels. Il s'agit du droit au respect de la vie privée avec notamment le droit au secret des correspondances et le droit à l'image.

Ces données étant, par nature, strictement personnelles, les proches du défunt ne peuvent, en principe, y avoir accès.

La jurisprudence du Conseil d'Etat

Le Conseil d'Etat a jugé en 2016, que « *des personnes ne peuvent, en leur seule qualité d'ayants droit de la personne à laquelle se rapportent les données, être regardées comme des personnes concernées* » au sens de la loi Informatique et libertés.

Dans une décision du 7 juin 2017, le Conseil d'Etat a précisé qu'il en va différemment lorsque la victime d'un dommage décède, son **droit à la réparation d'un dommage** étant transmis à ses héritiers.

En pareil cas, ils ont le statut de « **personnes concernées** » pour l'exercice du droit d'accès aux données personnelles du défunt ; mais uniquement « *dans la mesure nécessaire à l'établissement du préjudice que ce dernier a subi en vue de sa réparation et pour les seuls besoins de l'instance engagée* ».

Loi Informatique et libertés

Depuis sa modification en 2016 par la **loi pour une République numérique**, la loi Informatique et libertés prévoit, à son article 85, le droit d'organiser, de son vivant, par l'établissement de directives, la conservation l'effacement et la communication de ses données à caractère personnel après sa mort.

Ainsi, **une personne peut être désignée pour exécuter ces directives**. Celle-ci a alors qualité pour prendre connaissance des directives et demander leur mise en œuvre aux responsables de traitement concernés.

Ces directives sont :

- **générales** lorsqu'elles portent sur l'ensemble des données concernant une personne ;
- **particulières** lorsqu'elles ne concernent que certains traitements spécifiques.

Les directives générales peuvent être **enregistrées auprès d'un tiers de confiance numérique** certifié par la Cnil.

Les directives particulières sont enregistrées auprès des responsables de traitement concernés (réseaux sociaux, messageries en ligne). Elles font l'objet du consentement spécifique de la personne concernée et ne peuvent résulter de la seule approbation des conditions générales d'utilisation.

En l'absence de directives données de son vivant par la personne concernée, les héritiers qui justifient de leur identité ont la possibilité d'exercer certains droits, en particulier les droits :

- **d'accès**, dans la mesure nécessaire à l'organisation et au règlement de la succession du défunt ;
- **d'opposition** pour procéder à la clôture des comptes utilisateurs du défunt et s'opposer à la poursuite des traitements de données à caractère personnel le concernant ;
- **de rectification** pour demander au responsable de traitement de tenir compte du décès de la personne concernée et de procéder à la mise à jour de ses données.

Les fonctionnalités mises en place par les réseaux sociaux

Alors que près de 8.000 personnes inscrites sur Facebook décèdent chaque jour dans le monde et qu'à l'horizon 2069, Facebook pourrait comprendre plus de morts que de vivants, il est nécessaire de s'interroger sur la gestion *post mortem* des profils sur les réseaux sociaux.

La Cnil a fait un point sur le sort des données numériques des défunts.

La Cnil rappelle qu'actuellement, en l'absence d'une demande en ce sens de la part des héritiers ou des proches d'une personne décédée, un réseau social ne peut prendre l'initiative de supprimer un profil inactif. Les réseaux sociaux tels que **Facebook, Twitter ou LinkedIn** ont ainsi mis en place des outils de suppression ou de désactivation des profils des personnes décédées.

La Cnil liste, de manière non exhaustive, les **liens permettant aux proches d'entamer une procédure de signalement de décès** au site ou au réseau social concerné.

Par ailleurs, depuis quelques années, Facebook propose de **transformer le compte d'une personne décédée en « compte de commémoration »**. Cela permet aux proches de lui rendre hommage, de partager des souvenirs en lui offrant une sorte d'**immortalité numérique**. Les profils commémoratifs n'apparaissent pas dans les espaces publics de Facebook.

Ainsi, de leur vivant, les utilisateurs de Facebook ont la possibilité de :

- désigner un « contact légataire » qui gérera leur profil une fois celui-ci transformé en compte de commémoration ou ;
- demander à Facebook de fermer définitivement leur compte après leur décès.

Selon la politique d'utilisation et de confidentialité de Facebook, les informations de connexion au compte du défunt ne sont pas communicables.

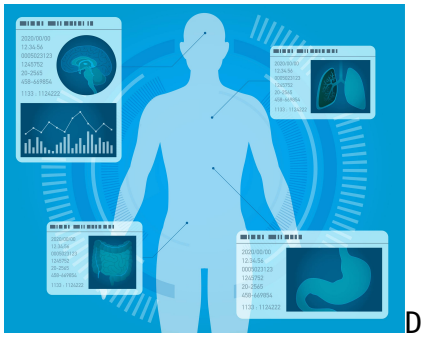
Les recours pour faire respecter les données numériques des défunts

La Cnil rappelle que, lorsqu'une personne s'estime lésée par le traitement de données concernant un proche décédé, elle peut **saisir les tribunaux** pour demander réparation du préjudice subi.

De même, les héritiers peuvent saisir les tribunaux lorsque l'utilisation des données d'un défunt porte atteinte à sa mémoire, sa réputation ou à son honneur ou tout autre préjudice.

Virginie Bensoussan-Brulé
Alexandra Guermonprez
Lexing Contentieux numérique

Projet de loi bioéthique : IA et données massives des patients



De nouvelles précisions s'agissant des **traitements algorithmiques de données massives** sont envisagées dans le projet de loi sur la révision des lois de bioéthique qui a été présenté en Conseil des Ministres le 24

juillet 2019 et sera débattu au Parlement en septembre 2019. Il s'agit de la **3ème révision des lois bioéthique en 25 ans**.

Selon le compte-rendu du Conseil des Ministres, « *cette révision des lois de bioéthique s'inscrit dans un contexte de sauts technologiques inédits, auxquels s'ajoutent des attentes sociétales fortes* ».

Droits et garanties des patients en matière de données massives introduits par le projet de loi

L'article 11 du projet de loi relatif à la bioéthique entend sécuriser la bonne information du patient lorsqu'un **traitement algorithmique de données massives** (« **intelligence artificielle** ») est utilisé à l'occasion d'un acte de soin.

Il introduit un nouvel article L.4001-3 dans le Code de la santé public, aux termes duquel le professionnel de santé devra **informer le patient** en cas d'utilisation d'un traitement algorithmique de données massives pour des actes à visée préventive, diagnostic ou thérapeutique, lorsqu'il communique les résultats de ces actes.

Il devra également informer le patient des « *modalités d'action* » du traitement de données.

L'article prévoit l'intervention du professionnel de santé pour réaliser l'adaptation des paramètres du traitement et rappelle ainsi l'**importance de l'intervention humaine dans le fonctionnement de l'intelligence artificielle**.

En outre, la traçabilité des actions d'un tel traitement algorithmique et des données utilisées dans le cadre de ce traitement sera assurée et les informations qui en résultent seront accessibles aux professionnels de santé concernés.

Ainsi, il s'agit de garantir la possibilité d'auditer les algorithmes, le respect des principes de transparence des algorithmes, de garantie humaine, et de traçabilité, lesquels constituent les **garanties nécessaires au développement de l'intelligence artificielle**.

Il faut « *garantir que l'intelligence artificielle augmente l'homme plutôt qu'elle ne le supplante et participe à l'élaboration d'un modèle français de gouvernance éthique de l'intelligence artificielle. Nous devons collectivement faire en sorte que ces nouveaux outils soient à la main humaine, à son service, dans un rapport de transparence et de responsabilité* », comme affirmé par Isabelle Falque-Pierrotin, ancienne présidente de la Cnil.

L'article 11 du projet de loi prend en compte les propositions du Comité consultatif national d'éthique (CCNE) dans son avis 130 adopté le 29 mai 2019 « **Données massives et santé : une nouvelle approche des enjeux éthiques** ». Dans cet avis, le CCNE formule notamment les propositions suivantes :

- « *toute personne a droit à une information compréhensible, précise et loyale sur le traitement et le devenir de ses données* » ;
- les résultats doivent être validés par une garantie humaine.

Droits des patients en matière de traitements exclusivement automatisés au titre du RGPD

Dans le cas où **une décision individuelle automatisée** serait fondée exclusivement sur le traitement automatisé de données massives, l'article 22 du Règlement européen sur la protection des données (RGPD) dispose : « *la personne concernée a le droit de ne pas faire l'objet d'une [telle] décision […] produisant des effets juridiques la concernant ou l'affectant de manière significative de façon similaire* ».

Cette disposition ne s'applique pas lorsque la décision :

- « *est nécessaire à la conclusion ou à l'exécution d'un contrat entre la personne concernée et un responsable du traitement ;*
- *est autorisée par le droit de l'Union ou le droit de l'État membre auquel le responsable du traitement est soumis et qui prévoit également des mesures appropriées pour la sauvegarde des droits et libertés et des intérêts légitimes de la personne concernée ; ou*
- *est fondée sur le consentement explicite de la personne concernée* ».

Dans la première et la dernière hypothèse, l'article 22 du RGPD prévoit l'obligation pour le responsable de traitement de mettre en œuvre « *des mesures appropriées pour la sauvegarde des droits et libertés et des intérêts légitimes de la personne concernée, au moins du droit de la personne concernée d'obtenir une intervention humaine de la part du responsable du traitement, d'exprimer son point de vue et de contester la décision* ».

Il est en outre précisé que les décisions correspondant aux trois hypothèses susvisées ne peuvent être fondées sur les catégories particulières de données visées à l'article 9 du RGPD, parmi lesquelles figurent les données de santé, sauf si des mesures appropriées pour la sauvegarde des droits et libertés et des intérêts légitimes de la personne concernée ne soient en place et que l'une des conditions suivantes est remplie :

- la personne a donné son **consentement explicite** ;
- le traitement est nécessaire pour des **motifs d'intérêt public importants**, sur la base du droit de l'Union ou du droit d'un État membre qui doit être proportionné à l'objectif poursuivi, respecter l'essence du droit à la protection des données et prévoir des mesures appropriées et spécifiques pour la sauvegarde des droits fondamentaux et des intérêts de la personne concernée.

Marguerite Brac de la Perrière
Isabeau de Laage
Lexing Santé numérique

RGPD Acte 2 : le cabinet participe à l'IT Tour 2018

Le cabinet participe à l'IT Tour 2018 organisé par Le Monde informatique autour des exigences IT, du RGPD et du Data Management.

« ***À la pointe de vos exigences IT*** » : tel est l'intitulé de cette nouvelle édition de l'IT Tour organisé par Le Monde informatique en région **du 26 septembre au 6 décembre 2018**.

L'IT Tour 2018 est un **évènement qui concentre l'ensemble des acteurs IT : DSI, RSSI, responsables informatiques et directeurs de la transformation numérique** ainsi que de prestigieux prestataires et éditeurs, pour aborder les tendances IT qui feront le système d'information de demain.

A l'occasion de trois étapes de l'IT Tour 2018 (Lille le 4 octobre, Reims le 8 novembre, Orléans le 6 décembre), un représentant du cabinet Lexing Alain Bensoussan Avocats participera à une table ronde consacrée au **Data management et aux enjeux liés au Règlement général sur la protection des données.**

Intitulée « RGPD Acte 2 : gagner en agilité et en conformité avec le Data Management », celle-ci abordera les points suivants :

- Bien préparer ses données, veiller à leur qualité ;
- Intégrer, exploiter et valoriser dans le temps ses données ;
- Les clés d'une gouvernance efficace des données.

La participation à l'IT TOUR 2018 est gratuite. Elle est réservée aux équipes IT (DSI, RSSI, chefs de projets…) des entreprises utilisatrices publiques ou privées.

Chacun des participants repartira avec le Guide RGPD acte 2 auquel a participé le cabinet Lexing Alain Bensoussan Avocats.

Pour retrouver le programme du IT Tour 2018 du Monde Informatique et vous inscrire : http://www.it-tour.fr.

Eric Bonnet
Directeur du Département Communication juridique

Le machine learning, déjà compositeur désormais cinéaste

 La création récente et inédite d'œuvres par des algorithmes soulève de nombreuses questions en droit d'auteur.

Alors que la musique composée par des programmes d'intelligence artificielle connaît ses premiers succès populaires, c'est désormais au tour du cinéma de faire appel aux techniques de machine learning.

Le machine learning, auteur compositeur

A l'automne 2016, Sony diffusait en ligne deux titres largement écoutés, composés par son programme de machine learning baptisé Flow Machines. Le premier, « Daddy's Car » (1), s'inspire directement du répertoire des Beatles, tandis que le second, « The Ballad of Mr Shadow » (2), est issu de l'étude des styles propres à Irvin Berlin, Duke Ellington, George Gershwin et Cole Porter (3).

Si plusieurs programmes informatiques étaient déjà parvenus à générer une création musicale originale (4), notamment au travers des travaux de David Cope (5) ou encore du TensorFlow de Google (6), c'est véritablement la première fois que des algorithmes d'intelligence artificielle parviennent à composer des œuvres aussi abouties.

Cette réussite s'explique tant par la performance des systèmes machine et deep learning développés aujourd'hui (7) que par les quantités considérables de données transmises à ces machines pour fournir un résultat optimal. C'est effectivement grâce à l'analyse d'un catalogue aussi vaste que celui des Beatles, et plus précisément de l'étude minutieuse des partitions, de l'orchestration et de la production de l'ensemble de leurs œuvres, qu'un modèle de machine learning a pu restituer une mélodie originale en tout point semblable à leur univers musical.

Le machine learning, réalisateur d'une oeuvre cinématographique

Désormais, les prouesses artistiques du machine learning ne se cantonnent plus à la musique, et c'est l'actrice américaine Kristen Stewart qui assure la publicité de l'utilisation de cette technologie au cinéma. A l'occasion de la présentation de son premier court métrage au festival de Sundance (8), cette dernière a en effet coécrit un article scientifique sur le recours au machine learning au sein

de son film « Come Swim » (9).

Elle y explique comment le machine learning a permis la création d'une œuvre originale, via le transfert d'un extrait cinématographique au sein d'une représentation picturale. La création finale a emprunté les mouvements et traits du film originaire, tout en ayant intégré l'atmosphère et les couleurs d'une œuvre figée. « Come swim » apparait de la sorte comme une œuvre composite (10), coréalisée par Kristen Stewart et un système de machine learning, reprenant le scénario d'un premier film, et dont la photographie au sens cinématographique est tirée d'une œuvre plastique.

Si dans la présente espèce, l'algorithme machine learning ne s'est appuyé que sur deux créations émanant du même auteur, également à l'initiative du programme, des difficultés importantes pourraient advenir dans les hypothèses d'une utilisation par la machine d'un nombre plus important d'œuvres issus d'auteurs différents. En pareille circonstance, et selon l'exploitation faite de ces œuvres par l'algorithme, il importera en amont de solliciter l'accord des différents auteurs, et ce conformément au régime juridique des œuvres dérivées (11).

Quelle protection accorder aux œuvres machine learning ?

Si ces œuvres restent aujourd'hui anecdotiques, car peu nombreuses et ne découlant pas toujours exclusivement de programmes d'intelligence artificielle, les questions soulevées par leur émergence et leur future expansion demeurent toutefois cruciales.

Il est tout d'abord primordial de pouvoir identifier le titulaire des droits d'auteur sur l'œuvre générée par le machine learning. Est-ce le concepteur du programme, son éventuel commanditaire ou la machine elle-même ? De la réponse apportée à cette interrogation découle l'attribution des différents droits et prérogatives rattachés à la qualité d'auteur. Pour une musique écoutée près de 1.500.000 fois sur YouTube cette réflexion est loin d'être anodine (1).

A cet égard, la jurisprudence a déjà eu l'occasion de préciser que la qualité d'auteur d'une œuvre de l'esprit ne peut être attribuée qu'à une personne physique. Le Tribunal de grande instance de Paris a par exemple refusé de reconnaitre un caractère original à des photographies aériennes, en précisant notamment que les clichés ont été pris à bord d'un avion équipé d'appareils photographiques déclenchés automatiquement et que l'angle de prise de vue était toujours le même (12). La Cour d'appel de Riom a quant à elle indiqué que la protection par le droit d'auteur d'une image satellite ne peut résulter que d'une mise en œuvre personnalisée d'une technologie complexe par un processus de transformation et d'amélioration (13).

Si les tribunaux semblent vouloir opérer une différenciation entre les œuvres de l'esprit protégeable par le droit d'auteur et les œuvres des machines, il serait opportun de réfléchir à un régime de protection venant davantage garantir l'investissement et définissant le titulaire de droits habilité à céder, concéder et défendre l'œuvre du machine learning. Face à ces questions éminemment sensibles, et partant du postulat que la création n'est plus l'apanage des êtres humains, il est aujourd'hui impérieux de déterminer le régime juridique des œuvres fruits de l'intelligence artificielle.

Lexing Alain Bensoussan Avocats
Lexing Propriété intellectuelle

(1) YouTube, Vidéo « Daddy’s Car: a song composed by Artificial Intelligence – in the style of the Beatles », 19-9-2016
(2) YouTube, Vidéo « Mr Shadow: a song composed by Artificial Intelligence », 19-9-2016
(3) Live Science, Article « Robo Rocker: How Artificial Intelligence Wrote Beatles-Esque Pop Song », 30-9-2016
(4) Wikipedia.org, Illiac Suite
(5) Theguardian.com, Article « David Cope: ‘You pushed the button and out came hundreds and thousands of sonatas' »,11-7-2010
(6) TensorFlow Google, Magenta
(7) Post du 6-2-2017
(8) Hollywoodreporter.com, Vidéo « Kristen Stewart (‘Come Swim’ Director) on Female Directors : « Just Make Stuff » Sundance 2017″, 1-2-2017
(9) Arxiv.org, Article « Bringing Impressionism to Life with Neural Style Transfer in Come Swim », 19-1-2017
(10) CPI, art. L. 113-2
(11) CPI, art. L. 113-4
(12) TGI Paris, 3e ch., 6-10-2009, Casalis c/ Ville de Paris
(13) CA Riom, ch. com 14-5-2003, Rubie’s france c/ Msat

Tribune pour un « Code civil » des données numériques

 Le Commissaire européen pour l’économie et la société numériques milite pour un «Code civil» des données numériques.

Lors de son passage à Francfort (Allemagne) le 16 octobre 2016 dernier, Günther H. Oettinger a lancé un appel à une action européenne pour encadrer la collecte, par les machines qui nous entourent, d’informations et données numériques.

En effet, l’ensemble des actions législatives en cours concernent le cas particulier des données à caractère personnel, soit les données d’identification directe ou indirecte des individus.

Ainsi, le Règlement Général sur la Protection des Données (UE) 2016/679 du 27 avril 2016 (« le RGPD ») entrera en vigueur en 2018. Le RGPD est le fruit de plusieurs années de travail et de réflexion qui vont permettre à l’ensemble des citoyens européens un meilleur contrôle de leurs données à caractère personnel. Ce texte présente aussi des apports importants pour les entreprises, qui auront dorénavant le bénéfice d’un guichet unique et d’un socle commun de règles européennes pour opérer sur le marché du numérique.

Malgré cette avancée, le Commissaire a mis l’accent sur une nouvelle

problématique : le traitement des données à caractère personnel ne constitue qu'une facette des enjeux du numérique.

La protection des données personnelles ne prend pas en compte l'évolution vers l'économie de marché dans lequel se situent les données numériques (1).

Les données collectées par des machines : l'or du futur

Nombreuses sont les données collectées quotidiennement qui ne sont pas des données à caractère personnel et dont le traitement est pourtant porteur de risques. Il s'agit des données collectées par des machines, qualifiées « d'or du futur ». Ce phénomène, s'il n'en est qu'à ses débuts, est voué à se développer de manière exponentielle.

A titre d'exemple, une voiture moderne est équipée de près de quarante microprocesseurs et de dizaines de capteurs contenus qui collectent des quantités de données numériques qui ne sont pas des données personnelles et qui présentent une valeur économique très élevée pour l'entreprise de par l'utilisation qu'elle peut en faire.

Défaut de réglementation

Il n'existe aucune réglementation en la matière à l'heure actuelle.

A défaut, les sociétés propriétaires de ces machines en profitent pour faire adhérer leurs utilisateurs à leurs conditions générales de vente et ainsi leur faire renoncer à leurs droits sur ces données.

Pour le Commissaire, cette pratique représente un réel manque à gagner que ce soit d'un point de vue politique ou économique. Ainsi, il souligne le réel bénéfice sociétal que pourrait offrir un accès élargi à ces données, couplé à l'utilisation du Big data.

Sur les données collectées par ces véhicules modernes, un accès élargi et enrichi pourrait par exemple permettre d'améliorer la gestion du trafic routier.

Le besoin d'une réglementation unifiée au niveau européen

Face à ces enjeux, il appelle donc à la clarification des questions qui peuvent se poser en matière de droits relatif à ces données, soulignant qu'un morcellement national des lois rendrait l'initiative inopérante sur notre marché unique.

Pour cette raison, pour le Commissaire, c'est au niveau européen que cette action doit être conduite.

Il semble donc qu'après la protection des données à caractère personnel, le prochain enjeu européen soit de parvenir à uniformiser la protection et la valorisation des données permettant de créer un nouveau marché contribuant à l'attractivité du continent européen.

Lexing Alain Bensoussan Avocats
Lexing Droit Informatique

(1) Règlement européen sur la protection des données, Textes, commentaires et orientations pratiques, sous la direction d'Alain Bensoussan, Lexing – éditions

Larcier.

La République numérique en marche : le projet de loi adopté


Mercredi 28 septembre 2016, le Sénat a adopté définitivement le projet de loi pour une République numérique.

Loi pour une République numérique : une loi audacieuse

La loi pour une République numérique est une loi audacieuse. Cette loi marque, au même titre que la loi pour la confiance dans l'économie numérique de 2004, l'évolution du droit du numérique (1). Cette loi a été portée brillamment par Axelle Lemaire, Secrétaire d'Etat chargée du numérique et de l'innovation.

L'élaboration même de la loi était marquée de nouveauté. La loi pour une République numérique est la première loi coécrite avec les internautes. Une première consultation a été menée par le Conseil national du numérique (2). Plus de 4.000 contributions ont été recueillies et ont permis au Gouvernement de définir une « Stratégie numérique » (18 juin 2015). Une consultation publique en ligne a permis ensuite à 21 330 contributeurs de déposer plus de 8500 arguments, amendements et propositions de nouveaux articles. Cette démarche consultative et participative est aujourd'hui généralisée.

Thématiques principales de la loi pour une République numérique

Cinq thèmes principaux sont portés par cette loi.

Thème 1 : la généralisation de l'open data par l'ouverture des données publiques

Ces dispositions s'inscrivent dans le prolongement de l'ordonnance de 2005 créant un principe de libre réutilisation des informations publiques. La loi pour une République numérique vient créer un principe d'open data par défaut (articles 1 à 9). Elle généralise l'ouverture des données publiques par leur mise à disposition sous forme électronique dans un standard ouvert. Elle introduit également la notion de données d'intérêt général (article 10 et suivants).

Thème 2 : le libre accès aux publications scientifiques et le droit d'exploration des données scientifiques

Les articles 17 et 18 bis de la loi pour une République numérique posent les principes fondateurs d'une Science ouverte. Elle permet aux chercheurs (recherche publique financée au moins pour moitié par des fonds publics) de mettre à disposition leurs publications scientifiques après le respect d'une période d'embargo. La loi introduit également une nouvelle exception au droit d'auteur autorisant l'exploration de texte et de données scientifiques à des fins de recherche publique, à l'exclusion de toute finalité commerciale. Le Livre blanc publié par le CNRS en mars 2016 « Une Science ouverte dans une République numérique » a appuyé et félicité ces dispositions.

Thème 3 : un renforcement de la protection des citoyens dans la société numérique

La loi pose le principe de neutralité du net (article 19) et de portabilité et récupération des données (article 21). Elle établit un principe de loyauté des plateformes et propose une définition de la notion de plateforme (article 22).

Thème 4 : la protection de la vie privée en ligne et le droit des données à caractère personnel

Le texte introduit également de nouveaux droits pour les individus en matière de données à caractère personnel. Le droit à l'oubli numérique pour les mineurs (article 32) ainsi que la confidentialité des correspondances privées (article 34) sont introduits. Des dispositions anticipent certains aspects du Règlement européen sur les données personnelles. Les pouvoirs de la Cnil sont renforcés.

Thème 5 : l'accès au numérique

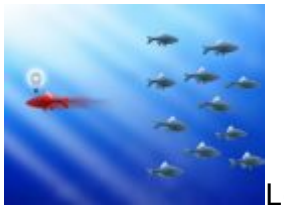
Ce thème est vaste et comprend notamment des dispositions relatives à l'accès des publics fragiles au numérique, le droit au maintien de la connexion ou encore le déploiement du très haut débit.

Des focus sur les dispositions phares de la loi pour une République numérique sont à venir.

Lexing Alain Bensoussan Avocats
Lexing Données publiques

(1) Sénat, Texte n°185 du 28-9-2016, Petite loi.
(2) Rapport du CNNum, Ambition numérique : pour une politique française et européenne de la transition numérique, juin 2015.

Marétique et logiciels d'analyse de données maritimes

 Le Big data de données satellitaires favorise le développement de logiciels d'analyse de données maritimes. Le traitement d'images satellitaires en mode Big data combiné à des logiciels d'analyse de données maritimes permet, de nouvelles applications très utiles à la navigation. Dans ce cadre le « booster » Morespace a été labellisé le 11 janvier 2016. Il a pour objet d'accélérer l'utilisation des données et techniques satellitaires dans le secteur maritime, en s'appuyant sur un vaste réseau d'acteurs sensibilisés à l'innovation et à l'entreprenariat (1).

Booster la technologie maritime par le logiciel d'analyse de données.

Stéphane Alain Riou, directeur adjoint du Pôle Mer Bretagne Atlantique animateur de ce booster, estime que « pour donner l'état de la mer, surveiller la qualité de l'eau, observer les flux de transports maritimes, conseiller la navigation…, on peut imaginer une foule de nouveaux produits ou services. Toutes les activités maritimes – plaisance, pêche, transport, aquaculture, etc.- dépendent étroitement de ces informations et prévisions (2)».

Morespace commandité par le Centre national d'études spatiales met en avant la croissance dans le domaine de l'analyse de données maritimes. Il éclaire également l'initialisation de nombreux projets de développement de logiciels d'analyse de données maritimes. De nombreuses offres présentent une gamme complète de prestations concernant l'analyse de données maritimes. Elles proposent des produits pour tous les domaines de la marétique, notamment des diagnostiques de contrôle et d'analyse de navire, des rapports de sinistre, l'optimisation de chantier naval, la gestion de la navigation.

Ces projets de logiciels d'analyse de données maritimes, reposent classiquement sur les technologies de traitement des images satellitaires actuellement « boostés » par les outils du Big data et même du Smart data. Pour ces projets complexes la qualification des équipes concernées, la détermination de spécifications techniques et fonctionnelles suffisamment détaillées et établies sur une expression de besoins claire est nécessaire.

Assurer la sécurité juridique du projet par l'outil juridique.

De plus dans ce domaine, il est préférable que des développeurs disposant d'une expertise maritime reconnue soient choisis pour réaliser ces projets. L'innovation technologique marétique étant constante, ils seront compétents pour assurer la scalabilité des logiciels d'analyse de données maritimes. La sécurité est également un paramètre fondamental dans le développement d'application utilisé dans le domaine maritime (3).

Le développeur devra pouvoir prendre en considération les spécifications techniques et fonctionnelles identifiées en interne par le client. Par exemple, dans ces projets, l'architecture de données doit être précise afin d'optimiser le stockage, le tri, l'intégration et l'utilisation des données. Pour cela un cahier des charges doit être rédigé. Il exprime de manière formalisée les besoins du client, oblige ce dernier à préciser sa demande, et permet au prestataire de mieux comprendre et appréhender le contexte et les contraintes à prendre en

compte. C'est sur la base de l'ensemble des informations contenues dans le cahier des charges que le prestataire s'engage à développer des logiciels d'analyse de données maritimes et que le client procède à leur réception.

Aux fins de mesurer, comparer et différencier les prestataires quant aux conséquences induites par leurs offres techniques et financières des prérequis juridiques pourront également être rédigés. Ils permettent de tenir pour acquis les réponses des prestataires aux prérequis juridiques, de faciliter et de rendre plus rapide la négociation des contrats, notamment pour les clauses de garantie ou de responsabilité qui sont en général des points bloquants.

Si ces facteurs clés de succès sont tous réunis, il ne peut y avoir aucun doute que les projets, notamment, initiés par Morespace permettront l'éclosion de produits et services rencontrant un vif succès.

Eric Le Quellenec
Daniel Korabelnikov
Lexing Droit Informatique

(1) Communiqué de presse COSPACE annonce Booster, en date du 11-01-2016, Ministère de la défense.
(2) Communiqué de presse, Le Pôle Mer Bretagne Atlantique lauréat de l'appel national à labellisation « Booster » sur l'utilisation des données spatiales, en date du 12-01-2016, disponible sur le site internet du PMBA.
(3) Cybersécurité & Marétique : un enjeu européen, Centre d'étude stratégique de la marine, 2014.

Management de la data sportive et patrimoine de santé

 Management de la data sportive et patrimoine de santé : « Faire du sport sera-t-il bientôt obligatoire ? »

Dans le cadre de la 7ème édition de Futur en Seine, le rendez-vous incontournable de l'innovation qui se tient à Paris et dans toute l'Ile-de-France jusqu'au 19 juin, le « Tribunal pour les générations futures » avait organisé le samedi 11 juin à la Gaîté lyrique un procès fictif autour du management de la data sportive avec comme thème : « Faire du sport sera-t-il bientôt obligatoire ? ».

Procès du management de la data sportive

Les applications et outils numériques permettant à chacun de mesurer ses données personnelles tendent à se démocratiser, avec la multiplication des sondes de data sportive, chaque individu apparaît sous forme de fichiers numériques, véritable

radio des pratiques sportives et du patrimoine de santé.

D'ailleurs certains assureurs proposent déjà de réduire le montant de leurs couvertures santé aux clients faisant du sport régulièrement. Une chose est sûre, les avantages du management de la data sportive personnalisée sont sans limites. De quoi laisser présager d'un futur dans lequel une forme physique optimale ne sera plus une simple option mais un acte citoyen. Bref, …

Faire du sport sera-t-il bientôt obligatoire ?

C'est en tout cas dans ce sens qu'a plaidé à cette occasion Alain Bensoussan qui s'est prononcé en faveur d'une « obligation de faire du sport afin d'améliorer les patrimoines de santé et d'allonger les durées de vie de tous les citoyens ».

Eric Bonnet
Directeur du département Communication juridique

Renseignement : traçabilité, conservation des données

 La traçabilité, la destruction et la conservation des données collectées sont précisées dans la proposition de loi.

C'est l'article 854-1 IV du Code de la sécurité intérieure qui permet de répondre aux exigences du Conseil constitutionnel

Dispositifs de traçabilité. L'interception et l'exploitation des communications feront l'objet de dispositifs de traçabilité définis par le Premier ministre.

Cependant, le régime des dispositifs de traçabilité n'est pas précisé par la proposition de loi (1).

Comme pour les communications nationales, les renseignements collectés feront l'objet d'une centralisation. La centralisation permettra à la Commission nationale de contrôle des techniques du renseignement (CNCTR) d'effectuer plus efficacement son contrôle.

Les communications internationales seront exploitées par les services spécialisés de renseignement. En pratique cela signifie que les opérations matérielles reposeront sur un ordre de l'exécutif.

Une différence est à noter avec le régime des interceptions de sécurité qui ne sont pas exploitées directement par les services de renseignement mais par un service du Premier ministre, le groupement interministériel de contrôle (GIC).

Conditions de destruction. Le projet d'article L.854-1 I du Code de la sécurité intérieure, prévoit que la destruction instantanée des communications échangées par des personnes utilisant des identifiants « rattachables au territoire nationale » (par exemple un numéro en 0033).

Conditions de conservation des données. La proposition de loi suit encore les exigences du Conseil constitutionnel en précisant dans le projet d'article L.854-1 du Code de la sécurité intérieure les conditions de conservation des données.

Il faut remarquer que ces durées de conservation sont augmentées par rapport à celles applicables à la surveillance des communications nationales.

Cette différence est expliquée par la Commission de la défense par des caractéristiques propres des communications internationales, essentiellement en langues étrangères, dont certaines peuvent être très rares.

La Commission de la défense précise également que dans de nombreux cas la surveillance des communications électroniques internationales est le seul moyen d'obtenir ou de confirmer des informations, alors que sur le territoire national des moyens complémentaires d'investigation peuvent être mis en œuvre.

Et enfin, la Commission de la défense indique que les données recueillies permettent très utilement de remonter a posteriori les parcours individuels, comme après un attentat ou une tentative d'attentat, et pour cela une certaine profondeur dans le temps est indispensable.

Les durées de conservation des données issues de la proposition de loi sont les suivantes :

- les correspondances sont conservées un an à compter de leur première exploitation dans la limite de quatre ans après leur recueil, contre trente jours à compter de leur recueil pour les correspondances collectées grâce aux interceptions de sécurité ;
- les données de connexion sont conservées six ans après leur recueil, contre quatre ans pour celles interceptées sur le territoire national ;
- la durée de conservation des renseignements chiffrés est portée à huit ans contre six ans sur le territoire national.

Tableau récapitulatif des durées de conservation des données

	Données de connexion (« contenants »)		Communications (contenus : correspondances et interceptions de sécurité)		Renseignements chiffrés	
	Territoire national	Surveillance internationale	Territoire national	Surveillance internationale	Territoire national	Surveillance internationale
Autorisation d'exploitation	4 mois renouvelables	1 an renouvelable	4 mois renouvelables	4 mois renouvelables		
Durée de conservation de données	4 ans à compter de leur recueil	6 ans à compter de leur recueil	30 jours à compter de leur recueil	1 an à compter de leur exploitation dans la limite de 4 ans après leur recueil	4 ans ou 30 jours à compter de leur déchiffrement dans la limite de 6 ans	6 ans ou 1 an à compter de leur déchiffrement dans la limite de 8 ans

Régime dérogatoire applicable aux communications mixtes. La proposition de loi décrit le régime relatif aux communications mixtes.

Une communication mixte est une communication qui met en jeu un numéro ou un identifiant rattachable au territoire national (numéros d'abonnement ou un identifiant technique).

Il faut retenir que le délai de conservation des correspondances court à compter de leur première exploitation, sans pouvoir excéder six mois à compter de leur recueil, contre trente jours à compter de leur recueil pour les correspondances collectées grâce aux interceptions de sécurité.

Didier Gazagne
Audrey Jouhanet
Lexing Cybersécurité – IE- Technologies de sécurité & Défense

(1) PLO AN 3173 du 28-10-2015.

Directive PNR : un transfert de données sous contrôle

La directive PNR sur l'échange des données personnelles des passagers aériens a été adoptée par le Parlement européen.

Alors que cette directive PNR faisait débat depuis cinq ans, les attentats

survenus en Europe en 2015 et début 2016 ont précipité son vote par le Parlement européen. Cette directive doit encore faire l'objet d'un vote formel des Etats membres au sein du Conseil de l'Union Européenne.

L'objectif de la présente directive PNR est de prévenir et de détecter des infractions terroristes et des formes graves de criminalité (1) ainsi que d'identifier des personnes qui n'étaient pas soupçonnées de participation à des infractions terroristes ou à des formes graves de criminalité (2).

A cette fin, la directive PNR prévoit la collecte et le transfert par les transporteurs aériens, des données des passagers (Passenger Name Record) de vols extra-UE aux Etats membres (3), c'est-à-dire des vols en provenance d'un pays tiers et devant atterrir sur le territoire d'un État membre ou en provenance du territoire d'un État membre et devant atterrir dans un pays tiers, y compris, dans les deux cas, les vols comportant d'éventuelles escales sur le territoire d'États membres ou de pays tiers (4).

Les données des passagers aériens seront centralisées, non pas sur un fichier unique à l'échelle européenne, mais sur une unité d'information des passagers (UIP) au sein de chaque Etat membre. Les Etats membres seront cependant libres de mettre en place conjointement une seule unité d'information des passagers aériens. Tous les pays de l'UE sont concernés par la présente directive, à l'exception du Danemark (5).

L'unité d'information des passagers sera chargée, dans chaque Etat membre, de collecter et d'analyser les données transmises par les transporteurs aériens et de les transmettre dans certains cas à d'autres Etats membres ou à des Etats tiers.

Cette obligation ne concerne que les vols extra-européens mais la directive laisse la possibilité aux Etats membres de faire rentrer dans son champ d'application les vols intra-européens et les vols charters. Dans ce cas, l'Etat membre devra le notifier à la Commission par écrit (6).

Les données collectées ne pourront en aucun cas porter sur l'origine raciale ou ethnique, la religion ou les convictions, les opinions politiques ou toute autre opinion, l'appartenance à un syndicat, la santé, la vie sexuelle ou l'orientation sexuelle d'un passager (7).

Elles ne pourront être utilisées que pour empêcher ou détecter des infractions terroristes et un nombre limité d'autres infractions graves, comme la pédopornographie et la traite d'êtres humain.

Par ailleurs, aucune décision ne pourra être prise concernant un passager aérien sur le simple traitement automatique de ces données PNR. Les évaluations effectuées à partir des données devront être « réexaminées individuellement par des moyens non automatisés » (8). Plus généralement, les autorités compétentes ne pourront prendre aucune décision produisant des effets juridiques préjudiciables à un passager ou l'affectant de manière significative sur la seule base du traitement automatisé de données PNR (9).

La durée maximale de conservation des données est fixée à 5 ans. Cependant les informations relatives à un passager aérien doivent être dépersonnalisées au bout de 6 mois, par le masquage des données permettant de l'identifier directement, telles que son nom, prénom, son adresse postale (10).

Enfin, pour s'assurer que les transporteurs aériens respectent leurs obligations de collecte et de transfert des données PNR, les États membres pourront prévoir des sanctions effectives, proportionnées et dissuasives, y compris des sanctions financières.

Par conséquent, et afin d'éviter de telles sanctions, il est nécessaire que les transporteurs aériens mettent en place une organisation interne leur permettant de répondre à leurs obligations en matière de collecte et de transfert des données des passagers aériens tout en veillant au respect des exigences en matière de protection des données personnelles, notamment des futures obligations du Règlement européen relatif à la protection des données (11), adopté le même jour que la présente directive PNR.

Lexing Alain Bensoussan Selas
Lexing Informatique et libertés

(1) Directive PNR (UE) 2016/681 du Parlement européen et du Conseil du 27 avril 2016 relative à l'utilisation des données des dossiers passagers pour la prévention et la détection des infractions terroristes et des formes graves de criminalité, ainsi que pour les enquêtes et les poursuites en la matière (JOUE L 119 du 4.5.2016, p. 132–149) considérant 6.
(2) Ibid. considérant 7
(3) Ibid. art. 1
(4) Ibid. art. 3, 2
(5) Ibid. considérant 40
(6) Ibid. art. 2, 1°
(7) Ibid. considérant 15
(8) Ibid. art. 6, 5°
(9) Ibid. art. 7, 6°
(10) Ibid. art. 12, 2°
(11) Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données) (JOUE L 119 du 4.5.2016, p. 1–88)

La gestion des données des applications abandonnées

 Polyanna Bigle est interrogée par le Groupe CGI (*) sur ce que doivent faire les DSI des données des applications abandonnées.

Certaines applications abandonnées au profit d'autres plus récentes et plus performantes, que faire des données qu'elles contenaient ? Maître Polyanna Bigle

répond que cela dépend du type de données concernées du point de vue légal car en effet ces archives peuvent constituer une preuve. L'entreprise doit donc prévoir au préalable un moyen de réversibilité, c'est-à-dire un moyen de récupérer les informations recueillies quelles que soient les applications abandonnées.

La principale raison à cette conservation nécessaire des données est qu'elles constituent bien souvent des preuves juridiques. La loi est même très précise quant à la durée de conservation de chaque type d'information. Par exemple, les documents comptables comme les factures doivent être conservés sur une durée qui peut aller jusqu'à dix ans. Mais si le droit précise des durées de conservation légales mais il ne donne pas encore d'indications sur la façon dont ces données doivent être conservées : il existe des normes d'archivage mais pas encore d'obligations.

« On trouve plusieurs normes d'archivage. L'exemple le plus connu est la norme NF Z 42-013 qui détaille une série de bonnes pratiques ». Parmi celles-ci : le cadre de l'archivage et des services de coffre-fort numérique. Sont ainsi listées les métadonnées (identifiant, date de création, etc.) à conserver pour chaque document numérique. « Ce sont pour l'instant des recommandations mais elles risquent de devenir obligatoires dans les prochaines années » estime Maître Polyanna Bigle.

Les données personnelles ont un traitement à part, le principe du droit à l'oubli, inscrit en 2004 dans la loi informatique et liberté, prévoyant la destruction des données nominatives une fois que le motif pour lequel elles ont été collectées n'est plus valable. Dans ce cadre, les entreprises sont tenues de supprimer les données quelle que soit la situation de l'application qui les conserve. C'est en partie pour cette raison que Maître Polyanna Bigle précise : « Les entreprises doivent mettre en place un système d'archivage et de purge des données sans attendre l'obsolescence des applications ».

Interview : « Applications abandonnées pourquoi garder les données ? », CGI Expert, 3 décembre 2015.

(*) Groupe CGI (Common Gateway Interface)

L'utilisation des données biométriques contenues dans les passeports

Dans un arrêt du 16 avril 2015, la Cour de Justice de l'Union Européenne a laissé entendre que les données biométriques contenues dans les passeports délivrés par les Etats-membres pourront être utilisées ou conservées à des fins autres que la délivrance du passeport (1).

Depuis quelques années la plupart les états européens intègrent des données biométriques sur la puce électronique des passeports, telles que la photographie numérisée du visage ou les empreintes digitales.

Le règlement (CE) n° 2252/2004 du Conseil européen impose, en effet, depuis le 13 décembre 2004, le prélèvement des empreintes digitales de toute personne demandant un passeport sur le territoire de l'Union Européenne.

Or, les données personnelles contenues dans un passeport biométrique sont des données sensibles, susceptibles de porter atteinte à la vie privée et à la protection des données à caractère personnel. La collecte de ces données permet pourtant de mieux lutter contre la fraude et l'usurpation d'identité.

Dans les affaires en cause, les requérants posaient une question préjudicielle à la Cour de Justice de l'Union Européenne portant sur le refus de délivrance par les autorités néerlandaises d'un passeport et d'une carte d'identité au prétexte que leurs données biométriques n'avaient pas pu être relevées.

Dans la première affaire, deux ressortissants contestaient le refus de délivrance d'un passeport au motif que ces derniers avaient refusé de fournir leurs empreintes digitales au moment de la délivrance du document.

Dans la seconde affaire était contesté le refus de délivrance d'une carte d'identité au motif que le requérant avait refusé de fournir ses empreintes digitales et sa photographie faciale.

Au soutien de leur demande, les requérants indiquaient que la saisie et la conservation des données constituaient une atteinte à leur intégrité physique et à leur droit à une protection à la vie privée.

En effet, lors de la fabrication des passeports les Pays-Bas conservent les données collectées dans une base de données. Les requérants considéraient cette opération contraire aux dispositions du règlement du 13 décembre 2004, qui prévoit à l'article 4 que « les éléments biométriques des passeports et des documents de voyage ne sont utilisés que pour vérifier l'authenticité du document et l'identité du titulaire ». Ces derniers craignaient que ces données sensibles soient utilisées à d'autres fins que la fabrication des documents d'identité, notamment, à des fins judiciaires ou qu'elles soient utilisées par les services de renseignement et de sécurité.

Dans la première affaire, la Cour a considéré que les cartes d'identité étaient exclues du champ d'application du règlement et que la question relevait par conséquent, de la législation nationale.

Dans la seconde affaire, la Cour a considéré que l'article 4 du règlement n'oblige pas les États membres à garantir, dans leur législation, que les données biométriques rassemblées et conservées ne seront pas traitées à des fins autres que la délivrance du passeport, un tel aspect ne relevant pas du champ d'application dudit règlement.

C'est ainsi que la Cour a considéré que cet article ne fait pas obstacle à ce que les données soient utilisées pour alimenter une base de données utilisée pour la fabrication des passeports.

En France, la Commission nationale de l'informatique et des libertés porte une

attention particulière aux conditions d'utilisation et de conservation des données biométriques collectées dans le cadre des demandes de délivrance de passeport et s'assure que celles-ci ne soient pas utilisées à d'autre fins comme par exemple, à des fins d'enquête policière.

Virginie Bensoussan-Brulé
Caroline Gilles
Lexing Droit Vie privée et Presse numérique

(1) CJUE 16 04 2015 C-446-12, Aff. jointes C-446/12 à C-449/12.

Perte de données et clause limitative de responsabilité

 En matière de contrats de maintenance informatique, le prestataire peut éviter d'engager pleinement sa responsabilité s'il perd les données de son client par l'effet d'une clause limitative à ce titre.

Perte de données et clause limitative de responsabilité. La validité d'une clause limitative de responsabilités pour perte de données a été analysée dans un jugement relatif aux contrats de maintenance informatique. Lors d'une intervention de maintenance d'un parc informatique, un prestataire a perdu les données sauvegardées sur les serveurs de sa cliente. En se référant au contrat, les juges ont appliqué la clause limitative de responsabilité et condamné la société de maintenance à indemniser sa cliente de la somme dérisoire de 7 280 €. Le préjudice réel était chiffré à 158 345,95 € (1).

La perte de données n'est pas, à elle seule, une faute lourde. Les juges auraient pu écarter la clause en considérant que la perte des données par la société de maintenance informatique constituait une faute lourde. Celle-ci est caractérisée par une négligence d'une extrême gravité confinant au dol et dénotant l'inaptitude du débiteur de l'obligation à l'accomplissement de sa mission contractuelle. Les juges ont considéré qu'aucun comportement exceptionnellement grave n'avait été démontré (2).

L'obligation essentielle du contrat doit être maintenue, même s'il contient une clause limitative de responsabilité. Les clauses limitatives sont appréciées de façon subjective, par référence aux circonstances de la clause. Les juges prennent en considération l'absence de contradiction entre la clause et la substance de l'obligation essentielle (3). Ce point n'a pas été retenu dans la décision rendue par le Tribunal de commerce Nanterre en mai 2014 (1).

La clause limitative de responsabilité pour les contrats cloud – Les conseils. Une obligation essentielle des contrats cloud est assurément que le

prestataire maintienne les données dans les serveurs sous sa responsabilité. Dans ce cadre, il est probable que la solution précitée diverge dans un contrat cloud. Cependant, plutôt que de discuter d'une telle clause devant un juge, il est préférable de le faire avant de signer tout contrat. En conséquence, pour être indemnisé à hauteur du préjudice subi, tout client souhaitant migrer ses données dans le cloud doit impérativement veiller à négocier soigneusement la clause écartant ou limitant la responsabilité du prestataire à ce titre.

Dans une perspective de nécessaire recherche d'un équilibre, le plafond de responsabilité doit être évalué en fonction des risques réels encourus et des incidences concrètes pour l'utilisateur. Il est conseillé de négocier avec soin les clauses responsabilité et préjudice et de prévoir un montant d'indemnité forfaitaire, évalué en fonction du risque réel. Le cabinet propose une démarche de type benchmark permettant de trouver la solution la plus adaptée.

Eric Le Quellenec
Daniel Korabelnikov
Lexing Droit Informatique

(1) TC Nanterre 2e ch. 2-5-2014.
(2) JTIT n° 152, 12-2014, p 5.
(3) Cass. com. 29-6- 2010 n°09-11841 Faurecia c. Oracle.

Vol de données : modification de l'article 323-3 du Code pénal

 La loi n°2014-1353 du 13 novembre 2014, renforçant les dispositions relatives à la lutte contre le terrorisme opère, par son article 16, un changement de rédaction de l'article 323-3 du Code pénal, permettant de réprimer le vol de données, sans toutefois recourir à la qualification de vol.

Institués par la loi dite « Godfrain », les articles 323-1 à 323-4 du Code pénal (1) prévoyaient cinq atteintes aux systèmes de traitement automatisé de données (bien connus sous l'appellation « STAD »), lesquelles sont :

- l'accès ou le maintien frauduleux dans le STAD ;
- l'action d'entraver ou de fausser le fonctionnement du STAD ;
- l'introduction frauduleuse de données dans un STAD ou la modification des données qu'il contient ;
- l'importation, la détention, l'offre, la cession ou la mise à disposition d'un équipement, d'un instrument, d'un programme informatique ou de toute donnée conçus ou spécialement adaptés pour commettre des infractions au STAD ;
- enfin, la participation à un groupement de pirates informatiques.

Cette troisième atteinte a été modifiée en novembre dernier afin d'intégrer dans son champ de répression l'inquiétant et récurrent vol de données, qui y échappait jusqu'alors.

L'ancien texte permettait, en effet, uniquement de condamner l'introduction, la suppression ou la modification frauduleuse de données dans un STAD… mais nullement leur copie. Pour combler ce vide juridique, plusieurs voies avaient été envisagées, parmi lesquelles la contrefaçon ou l'abus de confiance.

La qualification de vol qui semblait correspondre au mieux à la copie de données avait été, quant à elle, écartée, tant il était considéré (sans doute à juste titre) qu'il n'y avait pas soustraction frauduleuse d'une chose appartenant à autrui (2) :

- absence de soustraction, d'une part, puisque le légitime propriétaire des données les conserve et n'en est à aucun moment dépossédé (sauf hypothèse du vol de disque dur) ;
- absence de chose à proprement parler, d'autre part, puisque la soustraction vise un bien matériel pouvant être saisi physiquement (là où les données sont des biens immatériels).

Or, la loi pénale est d'interprétation stricte et la règle est d'or. Malgré les tentatives de la jurisprudence (3), la répression du « vol » de données se fait donc au détour de la qualification de vol (et de celle de recel), par l'ajout de quatre mots au texte de l'article 323-3 du Code pénal, en vigueur depuis le 15 novembre 2014, lequel réprime désormais, outre le fait d'introduire, de modifier et de supprimer, le fait « d'extraire, de détenir, de reproduire, de transmettre » frauduleusement des données dans un STAD.

La loi du 13 novembre 2014 vient ainsi sanctionner la copie frauduleuse de données, dans une optique de protection accrue de « l'économie de la connaissance ».

Virginie Bensoussan-Brulé
Annabelle Divoy
Lexing Droit pénal numérique

(1) L. n°88-19 du 5-1-1988 relative à la fraude informatique, insérant les articles 323-1 à 323-4 dans le Code pénal, en son Livre II « Des crimes et des délits contre les biens », Titre II « Des autres atteintes aux biens ».
(2) Comme l'exige l'article 311-1 du Code pénal, définissant l'infraction de vol.
(3) Cass. crim. 4-3-2008 n°07-84.002 Jean-Paul X Sté Graphibus.

Données numériques : une avancée vers un droit de propriété

 L'introduction d'un régime de propriété des données numériques (1) est primordial pour les entreprises.

La donnée numérique, en tant que chose incorporelle, a la particularité de pouvoir être reproduite à l'infini et à moindre coût, et ce sans jamais déposséder son propriétaire d'origine. Corollaire du principe de libre circulation des idées et des informations, la donnée est dite de manière traditionnelle de libre parcours. Or, la captation de données peut parfois causer à l'entreprise un préjudice important.

Plusieurs dispositifs légaux, en plus des dispositifs contractuels, permettent par exception au propriétaire de certaines données de se protéger d'une appropriation illicite :

- la lutte contre la concurrence déloyale ou le parasitisme économique ;
- la violation du secret de fabrique ;
- la protection de la vie privée et des données à caractère personnel ;
- la protection des données protégées par un droit de propriété intellectuelle ;
- le devoir légal de secret : secret médical, secret professionnel, secret de fabrication ;
- quelques décisions ont également reconnu le vol d'information.

La protection d'un « secret des affaires », en discussion devant les instances nationales et communautaires depuis plusieurs années, permettrait également de renforcer la protection des données industrielles et commerciales.

Toutefois, cette multitude de régimes juridiques ne permettent pas de protéger toutes les données sans distinction de valeur et de provenance. Leur application est également parfois complexe et source d'insécurité juridique.

Pour que la donnée soit protégée efficacement, il conviendrait de lui conférer un régime de protection de principe, en lui attribuant le statut de « chose » et en lui appliquant le régime du droit de propriété, droit universel et à valeur constitutionnelle, tel que prévu à l'article 544 du code civil :

- « La propriété est le droit de jouir et disposer des choses de la manière la plus absolue, pourvu qu'on n'en fasse pas un usage prohibé par les lois ou par les règlements. »

Plusieurs initiatives législatives ou décisions jurisprudentielles à travers le monde, Allemagne, Chine, Corée du Sud, Taiwan, USA, vont d'ailleurs dans le sens d'une application aux données des mécanismes traditionnellement associés à la propriété (régulation, taxation, commerce de bien virtuels).

L'article 16 de la loi n°2014-1353 du 13 novembre 2014 renforçant les dispositions relatives à la lutte contre le terrorisme est venu poser une première pierre à cet édifice de construction d'un régime de protection de la donnée.

Modifiant le premier alinéa de l'article 323-3 relatif aux atteintes aux systèmes de traitement automatisé de données, le texte dispose dorénavant que :

- « Le fait d'introduire frauduleusement des données dans un système de traitement automatisé, d'extraire, de détenir, de reproduire, de transmettre, de supprimer ou de modifier frauduleusement les données qu'il contient est puni de cinq ans d'emprisonnement et de 75 000 euros d'amende. »

Les termes « extraire, détenir, reproduire, transmettre » ont été ajoutés au texte initial. La notion d'extraction, en tant qu'action d'extraire, de « tirer, sortir une chose quelconque d'un endroit où elle est contenue » fait penser à la notion de « soustraction » utilisée dans la constitution du délit de vol (« soustraction frauduleuse de la chose d'autrui » article 311-1 Code pénal).

Ce régime de propriété des données, s'il voit le jour, ne devra toutefois pas être appliqué à toutes les données ; certaines données comme notamment la donnée scientifique étant par nature « un bien commun qui doit être disponible pour tous » , il conviendra d'organiser leur liberté d'accès dans le respect des enjeux de valorisation de la recherche.

Lexing Alain Bensoussan Avocats
Lexing Droit Propriété intellectuelle

(1) Alain Bensoussan, « La propriété des données », Blog expert Le Figaro, 18-5-2010 ; Didier Frochot, « Vous avez dit propriété des données ? », Les Infostratèges, 14-1-2011 ; David Barroux, Benoît Georges, Nicolas Rauline, « La propriété des données, défi majeur du XXI e siècle », Les Echos, 13-2-2014 ; Eric Gibory, « La propriété des données est un enjeu primordial », Le Figaro, 15-4-2014,
(2) Définition du terme « extraire » par le Centre National de Ressources Textuelles et Lexicales (CNRTL).
(3) Discours de Geneviève Fioraso, Secrétaire d'Etat à l'enseignement supérieur et à la recherche, auprès de la Ministre de l'éducation nationale, de l'enseignement supérieur et de la recherche, 24-1-2013, 5e journées Open Access.

Les bases de données et les objets connectés


50 milliards d'objets intelligents qui communiquent et combien de données collectées puis échangées par seconde ? Cette incommensurable masse de données produite par les objets connectés et regroupée sous l'appellation générique « big data » engendre une modification de leur appréhension et de leur contrôle : la base de données est virtuelle et alimentée en temps réel par les

données qui circulent et permettent aux objets d'interagir et de répondre à leur finalité.

Si disposer d'une information massive et facilement accessible peut être une force, elle ouvre également la voie à une multiplication des contentieux liés à la propriété des données et des bases, à leurs conditions d'exploitation et à leur fiabilité.

Protection et exploitation des données. Les données, en fonction de leur nature et donc de la qualification juridique qui en découle, sont régies des règles juridiques impératives qui influent sur les conditions de leur protection et les droits des tiers.

A titre d'exemples, les données publiques sont soumises aux dispositions de la loi Cada du 17 juillet 1978 qui a introduit un principe général d'accessibilité et de réutilisation des données publiques par les personnes privées et en fixe les conditions d'application. Les données qui émanent de personnes privées peuvent comporter des informations relatives à la vie privée ou encore comporter des éléments de savoir-faire d'une entreprise et font l'objet d'une protection spécifique à cet égard. Enfin, toutes peuvent également être protégées par le droit de la propriété intellectuelle : droit d'auteur, marques, dessins et modèles, etc.

Protection et exploitation des bases de données. Au-delà des données, les bases de données virtuelles créées grâce aux objets connectés peuvent en tant que telles être protégées.

Les bases de données bénéficient d'une double protection : par le droit d'auteur sur la structure de la base de données, sous réserve d'originalité (plan, rubriques, format, codes et libellés) et par le droit sui generis du producteur de la base de données.

Cette seconde protection du producteur de base de données, offerte à la personne qui prend l'initiative et le risque de l'investissement, lui permet d'interdire notamment l'extraction de la totalité ou d'une partie substantielle du contenu de la base et la réutilisation de la totalité ou d'une partie qualitativement ou quantitativement substantielle du contenu de la base, ainsi que l'extraction ou la réutilisation répétée et systématique de parties qualitativement ou quantitativement non substantielles du contenu de la base.

Ces règles doivent régir l'exploitation de données qui ne peut donc intervenir qu'après s'être assuré de l'origine des données concernées et, avoir lorsque les données sont privées, conclu une licence d'utilisation. Aucune extraction et/ou utilisation des données ne doit se faire en violation des droits du producteur de base de données.

Il ne s'agit toutefois que de l'état du droit. En effet, il n'est pas certain que ces règles traditionnelles trouvent à s'appliquer aux bases de données virtuelles créées grâce aux données collectées par les objets connectés, compte-tenu de la quantité de données échangées et des conditions de leur collecte.

Notamment, l'article L. 341-1 du Code de la propriété intellectuelle limite la protection du producteur de bases de données qui justifie que « la constitution, la vérification ou la présentation de celui-ci atteste d'un investissement financier, matériel ou humain substantiel ». Les cours et tribunaux accepteront-

elles d'accorder cette protection lorsque les données sont collectées par les objets connectés ?

Responsabilité. Enfin, l'identification légale d'un « responsable » des données assumant les risques et la responsabilité apparaît primordiale. Qui sera responsable d'une information erronée ou incomplète transmise par un objet ?

Ainsi, dans ce contexte virtuel et au-delà des enjeux liés à la protection des données à caractère personnel et à leur traitement, qui est propriétaire des données ? Qui en assume la responsabilité ? Qui décide de leur condition d'exploitation ?

L'enjeu est donc de taille : adapter les règles traditionnelles du monde moléculaire au monde virtuel afin que la propriété et les droits d'exploitation qui y sont attachés ne freinent pas le déploiement de nouveaux services.

Marie Soulez
Lexing Contentieux Propriété intellectuelle

Applications mobiles, protection des données et bonnes pratiques

Applications mobiles – Le 6 mai 2013, la Cnil a effectué un audit de 250 sites internet et applications mobiles régulièrement fréquentés portant sur l'information délivrée aux internautes. Cet audit a été réalisé dans le cadre de l' « Internet Sweep Day », en français, la « Journée de balayage de l'internet », première opération internationale d'audit coordonnée des autorités membres du Global Privacy Enforcement Network (GPEN).

Au total, près de 19 autorités compétentes en matière de protection des données personnelles ont évalué 2180 sites Internet ou applications les plus visités.

Les résultats de cette enquête ont montré l'insuffisance, voire parfois l'absence, d'une information claire des internautes sur les conditions de traitement de leurs données personnelles.

Ainsi, au niveau mondial, il a été constaté que 50 % des applications mobiles auditées ne délivrent aucune information à leurs visiteurs relative à la politique de protection des données personnelles. En outre, les mentions d'informations délivrées par les autres services sont apparues incomplètes, peu accessibles et peu compréhensibles.

Au point de vue national, il a été constaté que lorsque qu'elle est fournie, cette information n'est ni facilement accessible (pour près de la moitié des

sites et applications mobiles concernés), ni suffisamment claire et compréhensible (pour près d'un tiers des sites audités).

Or, les applications mobiles permettent une collecte de quantité d'informations ; ceci étant favorisé par le système d'exploitation, qui permet à certaines applications d'accéder, notamment par l'intermédiaire d'API, aux carnets d'adresses, aux contacts enregistrés par le propriétaire du portable ou encore aux photos ou de fournir des informations comme les identifiants uniques du téléphone.

Certaines applications utilisent également la géolocalisation par GPS ou encore par Wifi.

Compte tenu des caractéristiques de fonctionnement des applications mobiles, les principaux risques en matière de protection des données à caractère personnel proviennent de l'absence de transparence et l'absence de sécurité.

Aussi, il est nécessaire que l'ensemble des acteurs (magasin d'application, développeur d'applications mobiles…) prenne en compte, dès la conception de l'application, les contraintes juridiques relatives à la protection des données et qu'ensemble, ils adoptent une démarche de privacy by design. Cette démarche respectueuse de la protection des données, permettra également, dès la conception, d'identifier les développements et fonctionnalités nécessaires à la conformité, ce qui sera de nature à éviter d'avoir à développer, en fin de processus de création, des fonctions supplémentaires.

Dans le cadre du processus de création d'une application, les principes suivants devront être respectés, selon les recommandations du groupe de l'article 29 (1) :

- obtenir le consentement libre et éclairé de l'utilisateur préalablement à l'installation de données ou la récupération des données de son terminal,
- obtenir son consentement pour la géolocalisation, que celle-ci soit réalisée par GPS, ou wifi,
- proposer une politique de confidentialité lisible et compréhensible, accessible notamment depuis le magasin et au sein de l'application,
- respecter le principe de minimisation des données en collectant uniquement les données nécessaires à la réalisation de la finalité,
- déterminer une durée de conservation des données en tenant compte de la durée nécessaire à la réalisation de la finalité poursuivie et permettre à l'utilisateur de paramétrer les durées selon les données,
- mettre en place une procédure permettant à l'utilisateur de désinstaller l'application,
- informer le consommateur, conformément à l'article 32 de la loi Informatique et libertés, notamment des finalités poursuivies par les traitements de données et les destinataires de ces données,
- recueillir le consentement en cas d'utilisation de cookies, traceurs et autre device fingerprinting,
- mettre en œuvre une procédure permettant à l'utilisateur d'exercer effectivement les droits qu'il détient de la loi Informatique et libertés sans frais et de manière simple,
- tenir compte de l'âge des enfants et adopter selon cet âge une politique restrictive de traitement des données,
- prendre des mesures adaptées pour assurer la sécurité des données et veiller à ce que les prestataires, tels que les hébergeurs, garantissent la sécurité

et la confidentialité des données confiées.

Si l'objectif est d'assurer la protection des données des utilisateurs des applications mobiles, à l'instar de la démarche adoptée en particulier pour le Web avec la loi pour la confiance dans l'économie numérique, l'objectif est également d'adopter des comportements et des conditions d'utilisation propices à instaurer et maintenir la confiance des utilisateurs, sans laquelle il sera difficile de pérenniser le succès des applications mobiles.

Aussi, à tous ceux qui souhaitent se lancer, il est recommandé de bien définir les données qu'ils souhaitent collecter afin d'identifier précisément les contraintes juridiques existantes et les développements que cela implique tout en définissant et rendant accessible la politique de protection des données de l'application.

Céline Avignon
Lexing Droit Marketing électronique

(1) Groupe Article 29, Avis 02/2013 du 27-2-2013 ; Cnil, Rubrique Actualité, Article du 9-4-2013.

Le Big Data : Conférence vidéo pour Supinfo

 « Droit et Big Data » tel est le thème abordé par Alain Bensoussan devant les étudiants de SUPINFO, la Grande Ecole de l'informatique, du numérique et du management. Le mardi 02 avril, SUPINFO Nantes a eu l'honneur d'accueillir dans ses locaux Alain Bensoussan, avocat spécialisé en droit de l'informatique et fondateur de Lexing®, premier réseau international d'avocats technologues dédié au droit des technologies avancées. Au cours de cette journée, il est intervenu sur une thématique qui lui est chère et qui met en perspective les grands enjeux des nouvelles technologies du futur : « Le Big Data ».

« **Droit et Big Data** » : peut-on combiner droit et big data ?
Le terme Big Data s'est imposé en 2012 au sein des entreprises, à la fois dans les DSI, les départements marketing et Business Intelligence. Le phénomène Big Data suscite des investissements majeurs donnant naissance au développement d'une variété d'applications ou d'outils adaptés : Base de données orientée graphe, de framework comme mapReduce ou Hadoop et de systèmes de gestion de bases de données comme Big Table. Ce phénomène est considéré comme l'un des grands défis informatiques de la décennie 2010-2020 !

Il se présente en quatre parties :
– Première partie : les spécifications techniques ;
– Seconde partie: l'analyse Informatique et libertés ;

– Troisième partie : l’analyse comportementale ;
– Quatrième partie: le contrôle des données.

Conférence : L’ ère du Post-PC, une nouvelle ère ?


Emmanuel Walle était à l’édition des Matinales de l’innovation de Grand Paris Seine Ouest le 31 janvier 2013 sur L’ ère du Post-PC.

Un thème portant sur les aspects juridiques d’un nouveau mode de consommation des données de l’entreprise, des risques techniques et organisationnels (ATAWAD).

Une nouvelle ère, celle de l’après-PC, s’ouvre avec la convergence du design et de la fonctionnalité, de la mobilité et de la performance, des logiciels de bureau et de son univers personnel. Micro-ordinateurs, portables, tablettes, smartphones, téléviseurs, consoles de jeux… notre bureau se déplacera-t-il avec nous ?

L’événement avait lieu au Cube (20 Cours Saint-Vincent, 92130 Issy-les-Moulineaux) et était organisé par Seine Ouest Entreprise

Les Matinales de l’Innovation de Grand Paris Seine Ouest – L’ ère du Post-PC ? : Programme.

Apprivoiser et organiser le Cloud, question d’agilité


Apprivoiser et organiser le Cloud. Au cours d’un entretien accordé à Microactuel, Alain Bensoussan a abordé le Cloud en expliquant d’abord si nous devions avoir peur de perdre le contrôle de nos applications et données, puis le type de contrat à prévoir et enfin comment apprivoiser le Cloud.

Pour Alain Bensoussan, c’est avant tout une question d’agilité. Le Cloud

doit pouvoir donner une réponse à ce caractère anxiogène qu'est la peur de cette perte de contrôle.

La crainte est d'autant plus compréhensible que la législation informatique et libertés impose une extrême prudence à l'égard de la sécurité des données personnelles et des transferts, sous peine de sanctions pénales du vendeur.

Alain Bensoussan pour Microactuel, Novembre 2012.

Les FAI doivent garder vos données d'identification

 Le décret relatif à la conservation des données d'identification par les fournisseurs d'accès à Internet (FAI) et les hébergeurs est paru le 25 février 2011, soit plus de six ans après le vote de la loi qui avait instauré cette obligation (LCEN). Ainsi, depuis le 1er mars 2011, les hébergeurs de contenus et les FAI, pris dans leur fonction d'hébergeur de pages personnelles, doivent conserver les données d'identification des internautes.

Alain Bensoussan pour Micro Hebdo, le 19 mai 2011

Décret d'application sur la conservation des données d'identification

 Le décret d'application relatif à la conservation et à la communication des données permettant d'identifier les personnes ayant contribué à la création d'un contenu mis en ligne a été publié au Journal Officiel du 1er mars 2011. Le décret du 25 février 2011 précise l'ensemble des informations qui doivent être détenues et conservées par les fournisseurs d'accès et par les hébergeurs, conformément aux dispositions de l'article 6, II bis de la loi 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique (LCEN).

Les informations conservées diffèrent selon qu'il s'agit des fournisseurs d'accès ou des hébergeurs, à l'exception de celles qui sont fournies lors de la

souscription d'un contrat par un utilisateur ou lors de la création d'un compte et des informations relatives au paiement. L'ensemble des informations doit être conservé pendant une durée d'un an. Le point de départ de ce délai diffère selon les données.

Les fournisseurs d'accès doivent les conserver pour chaque connexion de leurs abonnés et les hébergeurs, pour chaque opération de création de contenu. Ce décret précise d'ailleurs que la contribution à la création de contenu comprend les opérations portant sur les créations initiales de contenus, les modifications des contenus et de données liées aux contenus ainsi que la suppression de contenus.

Enfin, ce texte est également venu fixer les modalités d'application relatives aux demandes administratives de communication qui sont prévues par les dispositions de l'article 6, II bis de la LCEN. Les surcoût éventuels supportés par les prestataires techniques pourront faire l'objet d'un remboursement par l'Etat dans des conditions déterminées par un arrêté ministériel.

Décret 2011-219 du 25 février 2011

Hadopi : de nouvelles mesures pénales imposées aux FAI

Le gouvernement vient de publier un décret qui précise que les opérateurs sont désormais tenus de relayer à leurs abonnés les emails d'Hadopi dans un délai de vingt-quatre heures, sous peine du versement d'une amende prévue pour les contraventions de cinquième classe (actuellement 1 500 €).

L'article R. 331-37 du Code de la propriété intellectuelle est ainsi complété par un alinéa visant à obliger tous les FAI (fournisseur d'accès à internet) à transmettre à leurs abonnés soupçonnés de téléchargement illicite, les emails émis par l'Hadopi dans les 24 heures.

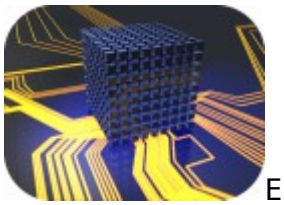
Un nouveau débat s'est cependant ouvert sur la validité de ce texte au regard du droit européen qui impose, au titre de la directive 98/48/CE, que le gouvernement notifie préalablement à la Commission européenne tout type de texte qui édicte des « règles techniques » visant les « services de la société de l'information ».

Il appartiendra au Conseil d'État, éventuellement saisi d'un recours en annulation, de se prononcer. Rappelons que, selon la jurisprudence de la CJCE (affaire CIA Security International), le défaut de notification préalable est sanctionné par l'inopposabilité du texte concerné.

Affaire à suivre…

Décret n° 2010-1202 du 12 octobre 2010

Conditions d'accès au fichier des renseignements généraux

 En principe, les fichiers des renseignements généraux (RG) ne peuvent faire mention de vos opinions politiques, religieuses ou syndicales sauf si vous êtes « fiché » pour atteinte à la sûreté de l'Etat ou à la sécurité publique (terrorisme notamment). Par ailleurs, un tel fichier fait partie de ceux dont les données ne vous sont pas directement accessibles. Ils sont soumis à un contrôle indirect exercé par la CNIL.
Seules les informations qui ne mettent pas en cause la sûreté de l'État et la sécurité publique, peuvent vous être communiquées par l'intermédiaire de la CNIL après accord du ministre de l'Intérieur. Ce dernier peut toutefois s'y opposer. Il doit alors motiver son refus. Ce refus peut être contesté devant le Conseil d'Etat. Ainsi, une personne ayant saisit la CNIL d'une demande d'accès aux informations la concernant contenues dans les fichiers des services des RG, a contesté devant le Conseil d'Etat la décision de refus de communication du ministre de l'intérieur. Cette haute juridiction a considéré que ce refus fondé exclusivement sur l'appartenance de cette personne à l'Eglise de Scientologie et sur la menace pour la sécurité publique que représentent les mouvements à caractère sectaire, était un motif « d'ordre général » qui n'était pas de nature à justifier un tel refus de communication. Le Conseil d'Etat a alors demandé au ministre de l'intérieur de réexaminer la demande d'accès de cette personne et a condamné l'Etat à lui verser la somme de 500 euros au titre des frais de procédures.

CE 28-7-2004 n° 243417