Caprioli & Associés
Société d'Avocats

Technologies, Information et Propriétés Intellectuelles

TIPI n° 23 – Eté 2014

L'édito de la TiPi

Car la protection des données à caractère personnel rime avec leur sécurité

Les évolutions du numérique telles les médias sociaux, le Cloud computing, le Big data, les objets connectés, Web 3.0 … pour la partie visible de l'iceberg, ont tout naturellement conduit à multiplier les collectes et les traitements de données personnelles, opérations dont le caractère intrusif n'est plus à démontrer mais à endiguer. Si de nouvelles opportunités s'ouvrent aux entreprises quant à la valorisation de leur patrimoine informationnel, des risques accrus s'en suivent, notamment au titre de la conformité légale (intrusion, divulgation, atteinte à la réputation, altération/perte de données, traitements non autorisés, etc.). Pour autant, on pourrait considérer que « *Tout est pour le mieux dans le meilleur des mondes possibles* » (merci Voltaire) car on a pu identifier les hommes de la situation : le RSSI, d'une part, qui devra efficacement œuvrer contre les risques plutôt techniques et le Délégué à la Protection des Données/DPD (sorte de « super CIL »), d'autre part, en tant que gardien du respect du cadre légal de protection des données.

De fait, actuellement, comme la loi « *Informatique et Libertés* » pose un **principe général de sécurité des données personnelles,** les politiques et les procédures à mettre en place en vue de garantir la sécurité et la confidentialité des données sont laissées à la libre appréciation des responsables, selon l'état de l'art et proportionnellement au niveau de sensibilité des données concernées. Or, force est de constater que le projet de réglementation sur la protection des données annonce une ère nouvelle quant aux exigences de sécurité. D'aucuns pourraient arguer du fait que le texte n'est toujours pas adopté et pas prêt de l'être au vu des centaines d'amendements et des divergences entre les versions de la Commission (2012) du Parlement (mars 2014) et du Conseil (juin 2014). En réalité, peu importe le sort du projet de Règlement car le LA est donné en matière de sécurité et partant : finie la fameuse obligation de moyen prescrite par l'article 34… Eh oui ! La tendance « analyse de risques » est définitivement vouée à s'appliquer à la mise en œuvre des traitements de données personnelles, quels que soient le secteur d'activités ou la taille de l'entreprise/organisme. Ceci étant, le principe de responsabilité (« *accountability* ») du projet de règlement, qui implique la mise en œuvre de mesures de protection efficaces des données permettant de garantir et de prouver la conformité légale des traitements de données dans la durée, n'est-il pas une déclinaison de principes et garanties applicables à la SSI ?

Dès lors et concrètement, que ce soit pour la constitution et le suivi de la documentation dédiée à la sécurité (sur l'analyse d'impact des traitements à mettre en œuvre sur la vie privée, l'étude de risques préalables, la notification des violations, les compte rendus d'audit, les mentions idoines des contrats impactant les données personnelles) ou pour la mise en place des procédures associées à l'Accountability », il semble que l'heure des supers héros a sonné : vive le RSSI et vive le DPD, et trinquons à l'alliance des deux fonctions qui comme tout bon mariage se prépare à l'avance.

Car somme toute, rappelons-nous que « *Ce qui est possible mérite d'avoir sa chance* » (Caligula - Camus).

Isabelle CANTERO
Juriste sénior,
Responsable du Pôle Données personnelles et vie privée

Aujourd'hui dans la TiPi :

Société d'avocats inscrite aux Barreaux de Nice et de Paris, SELARL au capital de 114.000 € inscrite au RCS NICE 442 341 319

9, Avenue Henri Matisse
06200 – NICE – Tél : (33) 04 93 83 31 31
Fax : (33) 04 93 83 50 49
contact@caprioli-avocats.com

29, Rue de Mogador
75009 – PARIS – Tél : (33) 01 47 70 22 12
Fax : (33) 01 47 70 22 56
contactparis@caprioli-avocats.com

site web : www.caprioli-avocats.com

Actualités

Le règlement européen sur l'identification électronique enfin adopté !

Le 3 avril 2014, le Parlement européen a adopté la proposition de règlement relative à l'identification électronique et aux services de confiance au sein du marché intérieur dit « eIDAS » (Electronic Identification and Signature). Ce texte est actuellement soumis à la lecture du Conseil pour validation. Ce règlement européen vient compléter la directive 1999/93/CE qui instaurait déjà un cadre juridique communautaire pour la signature électronique.

L'objectif de ce règlement est clair : **harmoniser les règles applicables en matière de services de confiance**, afin d'instaurer un climat de confiance pour le Marché unique électronique. Il s'agit, en effet, de **garantir une sécurisation des transactions électroniques au sein de l'Union européenne** (UE) tant pour les particuliers, les entreprises que pour les pouvoirs publics.

De manière générale, ce règlement vise **uniquement les systèmes d'identification électronique des Etats membres ainsi que les prestataires de services de confiance établis au sein de l'UE**. Autrement dit, les prestataires de services de confiance des Etats tiers sont exclus du champ d'application du texte.

En susbstance, ce texte introduit de **nouvelles définitions telles** que « *l'identification électronique* », le « *document électronique* », le « *cachet électronique* » et la « *signature électronique qualifiée* ». Sur ce point, l'adoption du règlement doit permettre une *uniformisation des termes juridiques* et garantir une plus grande sécurité juridique.

En outre, les Etats membres sont tenus à une **obligation de reconnaissance mutuelle des moyens d'identification électronique** étatiques uniquement (et pas les outils privés d'identification) pour ceux qu'ils auront décidés de déclarer.

Par ailleurs, le **régime de responsabilité des prestataires de services de confiance** électroniques est précisé.

Afin de sécuriser le choix des entités et des particuliers recourant à ces services, la proposition de règlement prévoit également la **création d'un label** « *services de confiance qualifiés* » qui se traduira par la **mise en place d'une marque de confiance à l'échelle européenne dès juillet 2015**. Ce label permettra **d'identifier les services de confiance offrant des garanties de fiabilité et de sécurité renforcées** (certificats de signature électronique qualifiés, horodatage électronique qualifié…).

Ainsi, le règlement EIDAS étant d'application directe, son adoption va permettre de soumettre tous les Etats membres de l'UE aux mêmes règles en la matière, source de sécurité juridique pour toute entité ou particulier procédant à des transactions électroniques au sein de l'UE. Toutefois, notons qu'il reste encore des actes délégués ou d'exécution à rédiger (actes techniques précisant les caractéristiques des services de confiance par exemple) par le CEN et l'ETSI et qui seront « endossés » par la Commission européenne.

Version adoptée accessible à l'adresse : http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P7-TA-2014-0282+0+DOC+XML+V0//FR&language=FR#BKMD-9.

Pour un article didactique, voir Eric A. CAPRIOLI et Pascal AGOSTI, *Identification électronique et services de confiance*, disponible à l'adresse : http://www.caprioli-avocats.com/identification-et-services-de-confiance. ;

Eric A. CAPRIOLI, *Signature électronique et dématérialisation* (Droit et pratiques), LexisNexis, 2014.

Le Décret OIV prévu par l'ANSSI se fait attendre

Si la loi n° 2013-1168 du 18 décembre 2013 relative à la programmation militaire (LPM) a été promulguée, il n'en demeure pas moins que son décret d'application est plus qu'attendu par les opérateurs d'importance vitale (OIV) comme les banques, les opérateurs de téléphonie, les infrastructures essentielles…

En effet, l'**article 22** de la loi prévoit un **renforcement des mesures de protection des OIV** d'une part, et **investit l'ANSSI de nouvelles prérogatives**, d'autre part. C'est notamment concernant l'étendue des obligations de détection et de déclaration mises à la charge des OIV que l'attente d'un décret se fait de plus en plus sentir.

Cet article astreint les OIV à une **obligation de détection des événements pouvant affecter la sécurité de leurs systèmes d'information (SI)**. A ce titre, les OIV sont tenus de mettre en œuvre des systèmes ou outils de détection qualifiés. Cependant, en l'état actuel, **la procédure de qualification des outils de détection et les prestataires proposant ce système ne reçoivent aucune définition**.

En outre, si les OIV ont **l'obligation de déclarer sans déla**i « *les incidents susceptibles d'affecter le fonctionnement ou la sécurité de leurs sytèmes d'information* », la loi ne définit toutefois pas les incidents visés par cette déclaration. Il résulte de cette absence de définition de la notion d'incident **une réelle insécurité juridique**, les OIV ne sachant pas dans quelle mesure se conformer à cette obligation de déclaration, dont le non respect peut donner lieu à des sanctions après mise en demeure. Dès lors, les contours de l'obligation de déclaration incombant aux OIV demeurant imprécis, l'action du pouvoir réglementaire s'impose dans un souci de sécurité juridique.

En dernier lieu, la loi reconnaît à l'ANSSI le **pouvoir de contrôler les systèmes d'information des OIV**, sur demande du Premier ministre, afin d'évaluer leur niveau de sécurité et de s'assurer du respect des mesures de sécurité prescrites à l'article **L. 1332-6-1 du Code de la défense** (mise en place d'outils de détection des failles). Ce contrôle des SI des OIV est également confié aux services de l'Etat. En conséquence, seul le Premier ministre est en droit d'ordonner aux OIV de se soumettre à un tel contrôle.

Les OIV devront donc encore patienter jusqu'en automne 2014, date à laquelle est prévue la publication du décret d'application.

Communication de l'ANSSI sur le projet de décret d'application de la Loi de Programmation Militaire, disponible à l'adresse : http://www.ssi.gouv.fr/fr/menu/actualites/l-anssi-s-attele-aux-decrets-d-application-de-la-lpm-portant-sur-la-protection.html

Projet de règlement Données à caractère personnel : la résolution du Parlement européen vient d'être adoptée

L'instauration d'un cadre juridique commun et harmonisé pour la protection des données à caractère personnel s'avérant indispensable au niveau européen, un projet de règlement a été proposé par la Commission européenne le 25 janvier 2012 et amendé – par la suite – par le Parlement européen. La résolution du Parlement européen, portant sur pas moins de 207 amendements, a d'ailleurs été adoptée le 12 avril 2014.

Concrètement ce projet de règlement est animé par la volonté de garantir aux personnes concernées deux droits fondamentaux, que sont le droit au respect de la vie privée et le Droit à la protection de leurs données personnelles, lors de la collecte et du traitement de telles données au sein de l'Union européenne.

Parmi les apports majeurs de ce projet de règlement dans sa version actuelle, on note :

- un **renforcement de l'obligation d'information** (clarté, précision et intelligibilié sont exigées) et **de recueil du consentement** incombant aux responsables de traitement (consentement libre, éclairé, exprès, spécifique et non équivoque de la personne concernée exigé) ;
- l'introduction d'un **principe de minimisation des données collectées** ;
- un **encadrement strict des transferts de données à destination d'Etats tiers** (autorisation préalable de l'autorité requise) et **des mesures de profilage** (droit d'opposition de la personne concernée) ;
- la **reconnaissance d'un droit à l'oubli numérique** pour les personnes ;
- **l'instauration d'un régime de responsabilité « *in solidum* »** des responsables de traitement et des sous-traitants ;
- et surtout **l'accroissement des pouvoirs de sanctions des autorités de contrôle** (amende de 100.000.000 d'euros, soit 5% du chiffre d'affaires annuel mondial)

Ce projet de règlement offre donc toutes les garanties nécessaires pour protéger effectivement les droits des citoyens européens, dont les données personnelles font l'objet d'un traitement.

Résolution du Parlement européen disponible à l'adresse : http://www.europarl.europa.eu/sides/getDoc.do?type=TA&reference=P7-TA-2014-0212&language=FR&ring=A7-2013-0402

Projet de loi égalité Hommes/Femmes : renforcement de l'obligation de dénonciation pour les intermédiaires techniques (art.17)

Le projet de loi portant égalité entre les femmes et les hommes adopté en seconde lecture par le Sénat le 18 avril 2014 **vient modifier le régime de responsabilité des intermédfiaires techniques,** visés par l'article 6-I de la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique, dite « LCEN ».

L'**article 17** du projet de loi, fort décrié, a finalement a été adopté. Cet article prévoit une **extension des contenus illicites** (faits d'incitation à la haine raciale en raison du sexe, de l'orientation sexuelle ou du handicap et diffusion d'images de violence) **soumis à l'obligation de signalement faite aux intermédiaires techniques**. Autrement dit, bien que les intermédiaires techniques ne soient aucunement tenus de surveiller les contenus qu'ils stockent au sens de l'article 6-I 7° de la LCEN, ils doivent néanmoins dénoncer aux autorités compétentes tous les contenus illictes qui leur seront signalés. Cependant, la liste des contenus visés ne cesse de s'allonger au détriment des intermédiaires techniques.

Projet de loi pour l'égalité entre les femmes et les hommes du 17 avril 2014, adoptée en seconde lecture par le Sénat, NOR : DFEX1313602L. http://www.senat.fr/petite-loi-ameli/2013-2014/444.html

De plus, ce renforcement de l'obligation de signalement des contenus illicites incombant aux intermédiaires techniques est d'autant plus dommageable qu'il aggrave leur régime de responsabilité. En effet, tout **manquement à cette obligation de signalement des contenus illicites est sanctionné pénalement (art. 6-I 7° de la LCEN)**. Or, l'appréciation de la licéité des contenus diffusés sur internet, exercice difficile, auquel doivent se livrer les intermédiaires techniques, incitera sans doute ces derniers à tous les signaler, afin d'échapper aux sanctions précitées. Dès lors, l'adoption définitive de ce texte en l'état conduirait inéluctablement à une aggravation du régime de responsabilité des intermédiaires techniques.

Focus

La dématérialisation des documents RH

Depuis la loi du 12 mai 2009 (1), les entreprises et les services en charge des ressources humaines commencent à proposer la dématérialisation des bulletins de paie et autres documents RH. Néanmoins, cette dématérialisation n'est pas encore un réflexe pour l'ensemble des salariés contrairement aux employeurs qui y voient la possibilité de réaliser des économies d'affranchissement ou encore des facilités pour la logistique et l'archivage. Un retour sur investissement (ROI) est attendu de ces nouveaux processus.

De plus, les DRH perçoivent, avec l'émergence des plates-formes de services et l'utilisation de logiciels en mode SaaS, le développement des applications mobiles ou encore le fait de doter de plus en plus de leurs salariés d'outils mobiles (ordinateurs, smartphones, tablettes....) l'utilité pour eux et leurs salariés de dématérialiser les documents RH. En effet, cette pratique a le mérite de faciliter les échanges « administratifs », de permettre aux représentants de la filière RH d'être plus disponibles et de privilégier la qualité de leurs échanges, le développement des compétences, la gestion des potentiels....

Les documents RH sont nombreux, notamment :

- les documents d'embauche ;
- le contrat de travail et avenants ;
- les bulletins de paie, déclarations sociales et déclarations d'accident du travail ;
- les attestations d'employeur ;
- les reçus pour solde de tout compte ;
- les avis de saisie sur salaire ;
- les fiches de postes (…)

C'est au travers du bulletin de paie et du contrat de travail (1), que seront identifiés les prérequis incontournables à la dématérialisation des documents RH (2).

1. Dématérialisation des bulletins de paie et du contrat de travail

La dématérialisation de ces documents suppose le respect de certaines dispositions légales et réglementaires.

1.1 Le bulletin de paie

L'article 26 de la loi n° 2009-526 du 12 mai 2009 n'impose aucune condition de forme pour la dématérialisation du bulletin de paie. Désormais, les entreprises peuvent délivrer à leurs salariés des bulletins de paie sous forme électronique à condition que :

- le salarié concerné **donne son accord**. La remise électronique des bulletins de paie est en effet subordonnée à un **accord individuel** de chaque salarié ;
- cette remise s'effectue **dans des conditions garantissant l'intégrité des données contenues dans le bulletin de paie.**

Comme les bulletins « papier », les bulletins dématérialisés devront être conservés par les employeurs **pendant cinq ans**. D'ailleurs, les articles L. 3243-2 et L. 3243-4 du Code du travail ont été aménagés en conséquence.

Au plan technique, le bulletin de paie électronique pose deux difficultés, la première tenant à **sa remise**, et la seconde, **à sa conservation**.

Concernant **la remise**, il convient de déterminer si le salarié doit accuser réception de l'envoi du bulletin de paie, ce qui permettrait à l'employeur de se préconstituer la preuve idoine.

(1) Loi n° 2009-526 du 12 mai 2009 de simplification et de clarification du droit et d'allègement des procédures, J.O. du 13 mai 2009, p. 7920 ; Eric A. Caprioli, *La dématérialisation des bulletins de paie*, Cahier de droit de l'entreprise n°4, juillet 2009, prat. 20.
V. Eric A. CAPRIOLI, *Signature électronique et dématérialisation* (Droit et pratiques), LexisNexis, 2014.

Compte tenu de l'évolution rapide des technologies, la loi n'a pas défini la formule «conditions garantissant l'intégrité des données ». Les débats parlementaires ont apporté quelques précisions en insistant sur la **sécurité de la conservation** de ces documents qui incombe à l'entreprise. La notion de «coffre-fort électronique » a été abordée, il s'agit d'un espace sécurisé (sous la forme d'un logiciel) destiné à assurer la conservation des bulletins.

Par ailleurs, la norme AFNOR NF Z42-025 sur les bulletins de paie électroniques recense les principes à observer en la matière. Ainsi, le **recours à un scellement du document, telle qu'elle est employée pour la facture électronique (cachet serveur),** constitue une garantie suffisante, mais non obligatoire. Il reste important de noter que le bulletin de paie n'est pas un acte juridique, mais une pièce justificative. Dès lors, les conditions entourant l'écrit électronique (articles 1316-1 et 1316-4 du Code civil) ne s'appliquent pas.

En conséquence, eu égard à l'ensemble de ces dispositions, la dématérialisation des bulletins de paie suppose :

- la mise en place d'un service d'archivage ou d'un coffre fort électronique (cf recommandation de la CNIL portant sur les coffres-fort numérique destinés aux particuliers (2)) ;
- le consentement du salarié ;
- la certification des données contenues dans le document ;
- l'identification de la durée de conservation du document ;
- la garantie de l'identité de l'émetteur du document ;
- l'intégrité du document pendant le temps de conservation nécessaire.

Néanmoins, les dispositions relatives au contrat de travail permettront d'identifier des prérequis complémentaires à ceux qui viennent d'être analysés.

1.2 Le contrat de travail

Le droit du travail français **n'impose aucun écrit pour le contrat à durée indéterminée**. Dès lors, il peut être conclu oralement et emporte tous les effets juridiques liés à un contrat à temps complet.

De nombreux accords collectifs exigent néanmoins un écrit. De même, la directive européenne du 14 octobre 1991 a étendu l'obligation pour tout employeur de mentionner par écrit, au moyen d'un contrat de travail, d'une lettre d'engagement ou de tout autre document, les éléments essentiels de la relation de travail avec le salarié.

Le document écrit, ainsi exigé, doit au moins contenir un certain nombre d'informations parmi lesquelles l'identité des parties.

Si aucune disposition spécifique relative au contrat de travail dématérialisé n'existe, il convient d'appliquer en la matière les dispositions du Code civil relatives au contrat électronique ou encore aux écrits électroniques.

Ainsi, conformément aux articles 1316-1 et 1316-4 du Code civil (ici applicables contrairement au bulletin de paie), la force probante de l'écrit électronique est identique à celle existant sur le support papier.

La jurisprudence considère que le contrat de travail est de nature particulière au regard de la preuve du droit civil Ainsi, en matière de droit du travail, **la preuve est libre comme en matière commerciale.**

(2) Délibération n° 2013-270 du 19 septembre 2013 portant recommandation relative aux services dits de « coffre-fort numérique ou électronique » destinés aux particuliers : http://www.cnil.fr/documentation/deliberations/deliberation/delib/297/ ;
Eric A. Caprioli, *La dématérialisation des bulletins de paie,* Cahier de droit de l'entreprise n°4, juillet 2009, prat. 20.

L'absence d'écrit étant fréquente, la jurisprudence a considérablement assoupli ces principes en admettant la preuve du contrat de travail par tous moyens (3). Ainsi, les juges ont retenu qu'un exemplaire unique du contrat de travail ou de la lettre d'engagement vaut commencement de preuve par écrit, tout comme la production de bulletins de paie (4).

Par conséquent, la preuve sous forme électronique peut être admise pour les contrats de travail au même titre que l'écrit sur support papier, **sous réserve de pouvoir identifier la personne dont il émane** et qu'il **soit établi et conservé** dans des conditions de nature à en **garantir l'intégrité**.

Compte tenu des spécificités attachées au contrat de travail, le respect des dispositions du Code civil susvisées s'impose afin de :

- **Identifier les parties :**

Les entreprises, qui souhaitent dématérialiser les contrats de travail, devront se doter **d'un procédé permettant l'identification des parties à la relation de travail**. On peut penser que le premier entretien en face à face, le plus souvent entre le futur salarié et l'employeur, pourrait être doublé d'une vérification d'identité, nécessaire à l'enregistrement du salarié si l'employeur entend prévoir l'émission d'un certificat d'identification à destination de ce dernier. D'autres stratégies d'identification sont envisageables.

- **Signer le contrat :**

Conformément à l'article 1316-4 du Code civil, la signature électronique permettra de **manifester le consentement au contenu du contrat de travail du salarié** (dûment identifié en amont). Toutefois, les entreprises devront prévoir de mettre à disposition cet outil de signature (par exemple, une fonctionnalité sur un compte intranet du salarié).

- **Etablir et conserver le document** dans des conditions de nature à en **garantir son intégrité** :

Différents procédés existent et permettent le respect de la chaîne de la confiance. Celle-ci doit être assurée de la création du document jusqu'à son archivage dans le coffre. A ce titre, **l'intégrité du document** devra être garantie pendant la durée de conservation légale ou conventionnellement définie entre les parties.

2. Les prérequis incontournables à la dématérialisation des documents RH

A travers ces deux exemples, il est possible de définir les règles suivantes pouvant être appliquées à tous les documents RH ou en tous les cas pour une bonne partie d'entre eux :

2.1 Identification nécessaire des parties à la relation contractuelle

La relation contractuelle dans une entreprise est certes établie entre l'employeur et le salarié. **Toutefois, la notion d'employeur doit être distinguée selon la taille de l'entreprise. En effet, le manager n'est pas toujours la personne qui assure les démarches RH.**

Par conséquent, il convient d'identifier les trois parties suivantes : le salarié, le manager et le RH en charge des démarches contractuelles et administratives, étant précisé que ces deux dernières peuvent évoluer pendant la relation contractuelle.

(3) Cass. soc. 27 juin 1990, n° 87-40.239.

(4) Cass. soc., 29 mai 1963, n° 62-40.786 : Bull. civ. IV, n° 438.

(5) V. Eric A. CAPRIOLI, *Signature électronique et dématérialisation* (Droit et pratiques), LexisNexis, 2014.

Conformément à ce qui a été développé ci-dessus, les moyens mis en œuvre doivent être assortis d'une technologie fiable (certifiée par l'ANSSI par exemple) afin de limiter les contestations.

2.2 Le consentement des salariés à la mise en place de la dématérialisation d'un document RH

Le consentement du salarié (y compris en tant que manager ou représentant de la filière RH), est obligatoire :

- tant **pour délivrer une identité numérique**, nécessairement couplée à l'identité des individus, notamment l'identifiant ou matricule RH ;
- que **pour la souscription par voie électronique des documents RH.** A ce titre, il est recommandé la **mise en place d'un espace numérique (comprenant un coffre-fort électronique par exemple)** offrant la possibilité à chaque salarié de cocher les documents qu'il souhaite établir et/ou recevoir par voie électronique.

La mise en place d'un tel système nécessitera pour l'entreprise de se conformer notamment aux **dispositions de la loi « *Informatique et libertés* » ou toute réglementation applicale.**

2.3 Un système fiable de modules entourant la dématérialisation

Quelque soit le document qui sera dématérialisé, il est impératif qu'il **soit intègre et infalsifiable de son émission jusqu'à son archivage.** Pour cela l'entreprise devra choisir de se doter de techniques ou de prestataires dont les pratiques sont fiables (certification) pour son système de dématérialisation tout en restant simple d'utilisation pour les trois parties utilisatrices sus-énoncées.

2.4 Un coffre-fort électronique pour conserver les documents dématérialisés

Ce dernier était déjà requis pour la dématérialisation du bulletin de paie (document que le salarié doit conserver quasiment à vie).

Les entreprises pourront donc utiliser ce système pour la conservation des autres documents RH du salarié **après avoir déterminé la durée de conservation de chacun d'eux.** Cette information pourra être issue soit des dispositions légales, soit être définie par accord collectif ou par engagement unilatéral de l'employeur.

2.5 Les étapes internes (et préparatoires) à la mise en place de la dématérialisation des documents RH

Lorsque une entreprise souhaite généraliser la dématérialisation des documents RH, outre le consentement de chaque salarié, une information/consultation des instances représentatives du personnel (comité d'entreprise et CHSCT) sera requise afin d'expliquer :

- les **éventuels impacts sur les conditions de travail** ;
- les **processus mis en place pour assurer la dématérialisation des documents** ;
- les **interfaces possibles (web, applications mobiles…)** ;
- la **sécurité des procédures** (droits d'accès, système d'acceptation, retour au papier…)
- les **modalités d'archivage durant la collaboration** ainsi qu'en cas de rupture ou de fin du contrat.

Jurisprudences

Blocage des sites internet contrefaisants : une simple obligation de moyens mise à la charge des FAI ? (CJUE 27 mars 2014)

Le 27 mars 2014, la Cour de Justice de l'Union Européenne (CJUE) s'est prononcée sur la **possibilité d'enjoindre aux fournisseurs d'accès à internet (FAI) de bloquer l'accès de leurs clients à des sites internet portant atteinte aux droits d'auteur.**

En l'espèce, des producteurs avaient saisi le juge des référés afin qu'il enjoigne à un FAI de bloquer l'accès de ses clients à un site proposant, sans leurs autorisations, le téléchargement ou le visionnage en streaming de leurs œuvres. Si en accédant à leurs demandes en première instance le juge avait précisé les mesures à adopter afin de procéder au blocage, les juges d'appel ont considéré que le FAI, certes soumis à une obligation de résultat, devait « *rester libre de décider des moyens à mettre en œuvre* ».

Le FAI contestant cette injonction s'est pourvu au motif que, d'une part, il n'est pas un intermédiaire au sens de l'article 8.3 de la directive 2001/29 et d'autre part, que « les *mesures de blocage susceptibles d'être mises en œuvre peuvent toutes être techniquement contournées et que certaines sont excessivement coûteuses* ». C'est à ce titre, que la CJUE a été saisie d'une question préjudicielle relative à l'interprétation de l'article 8.3 de la directive 2001/29.

Ainsi la Cour a d'abord affirmé que les **FAI étaient bien des intermédiaires au sens de l'article 8.3 de la directive 2001/29** c'est-à-dire, « *des intermédiaires dont les services sont utilisés pour porter atteinte à un droit d'auteur ou à un droit voisin* » et **à l'encontre desquels une injonction peut être délivrée**. La Cour a, en effet, estimé que le FAI est un *« acteur obligé de toute transmission sur internet d'une contrefaçon entre l'un de ses clients et un tiers, puisque, en octroyant l'accès aux réseaux il rend possible cette transmission »* et « *qu'exclure les FAI du champ d'application de l'article 8.3 diminuerait substantiellement la protection des titulaires de droit* ».

La CJUE a ensuite énoncé, après une mise en balance **des droits d'auteur et des libertés d'entreprise et d'information**, que les droits fondamentaux ne s'opposaient pas à une telle injonction générale dès lors que les **mesures prises *« ne privent pas inutilement les utilisateurs d'internet de la possibilité d'accéder de façon licite aux informations disponibles »* ; ont pour « *effet d'empêcher ou, au moins, de rendre difficilement réalisables les consultations non autorisées* »**, et de *« décourager sérieusement* **» les clients du FAI de consulter les œuvres protégées**.

La Cour déclare également que l'injonction générale ne semble pas porter atteinte à la substance même du droit à la liberté d'entreprise puisqu'elle *« **laisse à son destinataire le soin de déterminer les mesures concrètes à prendre** »* de sorte que le FAI peut adopter les mesures *« **les mieux adaptées aux ressources et aux capacités dont il dispose** »*. Elle ajoute, au demeurant, que ce type d'injonction permet au FAI de *« **s'exonérer de** **sa responsabilité** **en prouvant qu'il a pris toutes les mesures raisonnables** »* ce qui implique qu'il « ***ne sera pas tenu de faire des sacrifices insupportables.*** ». Enfin, la Cour souligne que **l'injonction doit être délivrée par un juge et confie le contrôle du respect des conditions énoncées aux autorités et juridictions nationales.**

Le FAI, intermédiaire au sens de la directive 2001/29 CE, doit donc prendre les mesures **nécessaires** afin d'interdire à ses clients l'accès à un site contrefaisant.

Arrêt de la CJUE du 27 mars 2014, « *UPC Telekabel Wien GmbH c/ Constantin Film Verleih GmbH* », disponible à l'adresse suivante : http://curia.europa.eu/juris/document/document.jsf?text=&docid=149924&pageIndex=0&doclang=FR&mode=lst&dir=&occ=first&part=1&cid=133650

Coup dur pour le Cloud : Microsoft tenue de communiquer aux autorités américaines les données de ses clients stockées à l'étranger

Le 25 avril 2014, la Cour fédérale du district de New York s'est prononcée sur la demande de Microsoft tendant à faire annuler partiellement un mandat de recherche et de saisie, délivré sur le fondement du « *stored communication act* » (SCA), qui exigeait qu'elle produise le contenu des emails de clients stockés sur un serveur à Dublin (Irlande).

Microsoft estimait que la référence du SCA à l'article 41 du code de procédure pénale (qui comporte une limitation de l'étendue territoriale du mandat) écartait la compétence des juridictions américaines pour délivrer un mandat de saisie et de recherche de données situées hors du territoire américain.

Le juge a tout d'abord précisé que le 4ème amendement (qui protège contre les perquisitions abusives aux domiciles des particuliers) ne trouvait pas à s'appliquer dans le cadre de perquisitions et de saisies de données, car **les serveurs ne constituent pas des domiciles virtuels à l'instar des domiciles « physiques »**. Il a alors expliqué que le SCA avait été notamment adopté afin d'offrir une protection constitutionnelle particulière aux recherches et saisies de données. Ce faisant, le juge a démontré que le mandat prévu par le SCA n'était pas un mandat traditionnel.

Dès lors, le juge a considéré qu'**ayant son siège aux Etats-Unis et en sa possession les informations recherchées, Microsoft se devait de les lui communiquer quand bien même les données seraient stockées en dehors du territoire américain**. Ce faisant, le juge n'a pu que rejeter la demande de Microsoft tendant à l'annulation partielle du mandat de recherche.

Cette décision rend donc la communication des données d'un prestataire Cloud américain totalement indépendante de leur lieu de stockage. Seul le critère du lieu d'établissement de la société semble dorénavant pris en compte. Cette décision va donc appeler à la prudence et à la réflexion des clients des prestataires Cloud américains, notamment en cas de stockage de données d'une certaine sensibilité.

Arrêt de la Cour Fédérale de New York du 25 avril 2014, *"Microsoft Corporation Vs JAMES C. Francis IV United States Magistrate Judge"*. Arrêt de la Cour Fédérale de New

Vie du Cabinet :

Le Cabinet souhaite la bienvenue à **Nathalie ANZIANI** dans la profession d'avocat et toute la réussite qu'elle mérite pour elle et son Cabinet **NewLaw**.

De plus, le Cabinet vient de rejoindre le **réseau JURIS DEFI** fondé en 1992, et qui regroupe des professionnels du droit (avocats, notaires, administrateurs et mandataires judiciaires) répartis sur l'ensemble du territoire.

Concours :

Ode à la Dématérialisation et à la Signature électronique

Le Cabinet a organisé un concours portant sur une définition poétique de la signature électronique et/ou de la dématérialisation dont le terme a été fixé au 21 juin 2014. Les envois furent nombreux et les membres du Comité de lecture furent enthousiastes pour plaider pour chacun de leurs coups de cœur. Après une longue concertation – difficile et passionnée, le lauréat du concours, qui recevra **l'ouvrage « Dématérialisation et signature électronique » d'Eric CAPRIOLI, dédicacé par ce dernier, est…**

Mr Ronan BRETEL, dont la prose figure ci-dessous :

Dématérialisation : *nom féminin* - Action longtemps rêvée, désormais dans l'espace des possibles. Elle fût longtemps la clef des songes, le passage dans l'au-delà, l'élévation au divin ou à la transcendance. - Elle permet désormais à l'Homme de s'affranchir de sa condition matérielle, mortelle et finie pour rejoindre un 'outre-part', au-delà des contraintes du réel, dépassant la substance mais la présupposant

pour se réaliser - l'Homme n'ayant désormais pour seule limite que ce qu'il peut imaginer.

Signature électronique : *nom féminin* - Vestige de la condition matérielle de l'Homme. Tantôt grâvée ou griffonnée, elle est désormais numérisée dans un monde de données. Marque du sujet dans un monde d'objets, subjectivisation de l'objectif, corps certain dans le fongible. Témoin de l'individuel dans le collectif. Propriété dans le monde partagé. Réalité précaire et finie de l'Homme dans l'espace de l'immatériel infini.

Quatre autres textes ont été sélectionnés et figureront sous peu sur le site du Cabinet : www.caprioli-avocats.com.

Le Cabinet tient à remercier vivement tous les participants pour avoir partagé leur talent et leur propre vision du Numérique.

Note bibliographique

La Banque en Ligne et le Droit – Cabinet CAPRIOLI & Associés – RB éditions –2014

La banque en ligne est une réalité de plus en plus prégnante dans les différents établissements bancaires et financiers en France. A côté des traditionnels services de consultation des comptes en ligne, d'impression de RIB, de virement… sont en train d'émerger de nouveaux services plus interactifs, les établissements bancaires et financiers multipliant les fonctionnalités offertes par l'Internet pour contractualiser à distance toujours plus de produits différents : contrat de crédit à la consommation, contrat d'ouverture de compte, contrat de fourniture de moyens de paiement, etc.

Bien évidemment, les autorités de régulation du secteur bancaire (comme l'ACPR), mais aussi d'autres autorités (comme la CNIL, l'AMF, la DGCCRF ou Tracfin) sont concernées. Ainsi, un cadre complexe de réglementations (Code monétaire et Financier, Code de la consommation, Code civil, Règlement CRBF 97-02, Loi Informatique, Fichiers et Libertés…) tend à s'appliquer de manière souvent complémentaire, parfois antagoniste.

Cet ouvrage a pour vocation d'expliquer de manière didactique les enjeux juridiques de la Banque en Ligne.

Conférences – Formations :

Revue Banque, *Archivage électronique et Coffre Fort, Rencontre Banque et Droit,* sous la direction d'Eric A. CAPRIOLI, 30 septembre 2014, Paris, www.revue-banque.fr .

Convention Nationale des Avocats, *La dématérialisation des Cabinets d'avocats*, Eric A. CAPRIOLI, 28 octobre 2014, Montpellier.

Forum ATENA, *Le règlement eIDAS*, Eric A. CAPRIOLI, 19 novembre 2014, Paris.

EFE, *La sécurité des données professionnelles à l'épreuve de la connectivité personnelle des salariés,* Eric A. CAPRIOLI, 26, 27 novembre 2014, Paris.

La minute nécessaire…

Le temps, le Droit et le Numérique

Traditionnellement, lorsque le juriste s'interroge sur la notion de temps, il y voit en premier lieu une portion de durée qui sera déterminée soit par la loi, le juge ou le contrat. Ces durées correspondent par exemple à la prescription civile (5 ans selon le droit commun), à une astreinte ou une exécution judiciaire ou encore à la durée d'une convention ou d'un préavis. En second lieu, le temps sera synonyme d'un moment, d'une date. Or, la date d'une loi, d'un jugement, d'un contrat ou d'un fait juridique renvoie à la notion de jour, c'est à dire l'espace de temps de 24 h qui s'échelonne de minuit à minuit. Ainsi, les délais sont calculés en jour, les actes juridiques mentionnent une date (jour, mois et année) de signature voire une date d'entrée en vigueur, les faits s'établissent au jour J (jour de survenance d'un dommage). Pour l'anecdote, il n'y a que l'état civil qui mentionne l'heure de naissance.

Dans un environnement numérique, les procédés de datation électronique (horodatage/timestamping) associent une date et un instant à un événement ou à une suite de données numériques, soit juridiquement, à un fait ou à un acte. La datation électronique issue des machines peut être beaucoup plus précise que le temps mesuré par l'homme étant donné qu'elle peut s'établir en jour, heure, minute, seconde, ou microseconde. L'horodatage est souvent utilisé pour les journaux d'évènements informatiques ou dans le cadre des documents signés électroniquement où l'on a recours aux services d'une autorité d'horodatage (timestamping authority), fondés sur une politique du même nom (ex : RGS V. 2 ou le RFC IETF 3161).

Par ailleurs, avec les échanges sur les réseaux numériques, on a pu constater depuis une vingtaine d'années une contraction de l'espace-temps : accélération du temps d'accès, de diffusion et de transmission des informations et abolition des distances et des frontières géographiques. Les communications via les réseaux sociaux et les équipements mobiles illustrent parfaitement ce phénomène et en amplifient la portée. L'instantanéité et l'universalité sont devenues les normes pour les caractéristiques fondamentales des communications du XXIème siècle.

Ceci n'est pas sans conséquence sur le plan judiciaire. En effet, si l'on prend l'exemple des atteintes à la e-réputation d'un individu ou d'une entreprise, force est de constater que la réponse est à tout le moins aléatoire, voire une mission impossible en raison de la diffusion quasi-instantanée sur toute la planète d'une information qui va nuire à l'image ou à la réputation d'une personne (physique ou morale). Certes le droit français dispose de textes en droit pénal ou civil pour réprimer ces délits, dont un nouveau délit relatif à l'usurpation d'identité (article 226-4-1 du code pénal), mais leur effectivité reste souvent hasardeuse dès lors que l'on sort des frontières de France ou de l'Union européenne. Pour agir contre le délinquant, il est impératif de l'identifier. Si la diffusion (planétaire) s'inscrit dans une très courte durée (moins de une minute), la réponse judiciaire, qu'elle soit civile ou pénale, dure un temps certain qui se compte, a minima, en jours, mois, ou années. Ces quelques éléments permettent de constater que le temps du droit n'est pas le temps du numérique, tant s'en faut !

Cette rubrique est un espace d'échanges. N'hésitez pas à nous contacter à l'adresse suivante : contact@caprioli-avocats.com

TiPi dans le détail :

La Newsletter du Cabinet Caprioli & Associés est une publication du Cabinet Caprioli & Associés.

La Newsletter est un instrument d'information et son contenu ne saurait en aucune façon être interprété comme un avis ou un conseil juridique.

Néanmoins, pour de plus amples détails sur un des thèmes abordés, ainsi que pour toute demande de désinscription à la présente Newsletter, n'hésitez pas à nous contacter à l'adresse suivante : contact@caprioli-avocats.com