L'édito du TiPi :

Du tourbillon quotidien aux méditations estivales (enfin presque !)

Affaire Kerviel, usurpation d'identifiants, développement des applications sans contact, iPad après iPhone et autres iPod, réseaux sociaux en évolution constante, lancement d'un label IdéNum pour les systèmes d'authentification, Hadopi 1, 2 et ?, proposition de loi modifiant la loi Informatique et Libertés, hébergeurs et web 2.0, cloud computing, notification des failles de sécurité, droit à l'oubli, les 10 ans de la loi sur la preuve et la signature, jeux et paris en ligne, obligations essentielles dans les contrats informatiques, etc.

L'actualité des technologies de l'information et des propriétés intellectuelles est en perpétuel devenir. Le temps s'accélère toujours plus vite au point que l'on a à peine le temps (si l'on peut dire) de s'arrêter sur une innovation technologique, une jurisprudence, un texte législatif ou réglementaire. Réflexions éphémères sur une invasion d'informations planétaires.

Après les pluies et les nuages islandais du printemps, on ne peut que souhaiter souffler avec l'indolence des beaux jours et du soleil du midi plein qui réchauffe les cerveaux agités de nos gouvernants et autres hommes de média. Il est temps de se poser et de prendre un recul suffisant sur les affaires en cours.

Le juridique va redevenir (enfin !) méditatif, l'espace de quelques semaines pendant les vacances judiciaires et parlementaires et une phase de repos sans doute bien méritée.

En ce 24 juin, date de la Saint Jean d'été, on ne peut que souhaiter l'apaisement et la joie, jusqu'à la rentrée des classes que l'on sent déjà poindre avec le déclin du soleil.

Courage, c'est déjà demain ! L'espace-temps d'un TiPi …

ERIC A. CAPRIOLI
Avocat à la Cour

Aujourd'hui dans le TiPi :

Actualités :

Procédure civile et communication par voie électronique

Le décret n° 2010-434 du 29 avril 2010 vient énoncer « *Vaut signature, pour l'application des dispositions du code de procédure civile aux actes que les auxiliaires de justice assistant ou représentant les parties notifient ou remettent à l'occasion des procédures suivies devant les juridictions des premier et second degrés, l'identification réalisée, lors de la transmission par voie électronique, selon les modalités prévues par les arrêtés ministériels pris en application de l'article 748-6 du code de procédure civile.* ». Ainsi, afin de poursuivre le développement de la communication électronique à travers les expérimentations en cours, l'identification réalisée, lors de la transmission par voie électronique, selon les modalités prévues par les arrêtés pris en application de l'article 748-6 du Code de procédure civile, vaut signature. Si l'identification, au sens de l'article 1316-4 du Code civil, est une fonctionnalité reconnue à la signature électronique, la manifestation du consentement ainsi que l'intégrité du document en sont d'autres, qui ne sont pas reprises par le décret.

Décret n° 2010-434 du 29 avril 2010 relatif à la communication par voie électronique en matière de procédure civile, J.O. du 2 mai 2010.

Cette mesure est provisoire et sera valable jusqu'au 31 décembre 2014. Cela crée une incohérence dans le domaine de la signature électronique – alors qu'elle commençait à peine à se structurer dans le domaine judiciaire avec le RPVA (pour les avocats) et le RPVJ (pour la justice).

Publication de l'arrêté portant approbation du Référentiel Général de Sécurité

Dans la dernière TiPi, il avait été indiqué que le décret fixant les conditions d'élaboration et de publication du RGS avait été publié le 4 février dernier et qu'un arrêté était attendu pour lui conférer ses effets juridiques. C'est désormais chose faite. L'arrêté du 6 mai 2010 portant approbation du Référentiel Général de Sécurité (RGS v. 1.0) et précisant les modalités de mise en œuvre de la procédure de validation des certifications électroniques a été publié au Journal officiel.

Arrêté du 6 mai 2010 portant approbation du référentiel général de sécurité (RGS) et précisant les modalités de mise en œuvre de la procédure de validation des certifications, J.O. du 18 mai 2010, p. 9152.

Les règles énoncées dans le RGS devront être appliquées :

- dans un délai de trois ans à compter de la publication de l'arrêté pour les téléservices et systèmes **en cours d'activité** ;
- dans un délai d'un an pour **ceux en cours de réalisation** ;
- et d'emblée pour les téléservices et systèmes qui seront déployés **après octobre 2010**.

Plusieurs de ces dispositions sont déjà mises en œuvre par les autorités administratives dans le cadre de téléservices existants mais aussi par des acteurs privés. L'ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information), qui dispose de toutes les compétences et de l'expertise nécessaires, assistera les autorités administratives qui le souhaiteront dans la mise en œuvre du nouveau dispositif.

Nouvelles clauses contractuelles types pour les transferts de données à caractère personnel

La Commission européenne a adopté le 5 février 2010 un nouveau jeu de clauses contractuelles types (CCT) pour réglementer l'externalisation croissante des traitements de données à caractère personnel. **Ce nouvel instrument vient en remplacement des CCT adoptées par la décision de la Commission du 27 décembre 2001. Ainsi, la Commission entend régir les situations de sous-traitance ultérieure qui ont lieu dans les pays tiers ne garantissant pas un niveau de protection adéquat au sens de la directive 95/46/CE.**

Conformément à la clause 11, l'importateur de données ne peut sous-traiter qu'après information préalable et accord écrit de l'exportateur. **Le pendant de cette exigence est l'obligation pour l'exportateur de données de tenir une liste à jour de l'ensemble des accords de sous-traitance ultérieure notifiés par l'importateur de données.** La sous-traitance ultérieure ne peut donc s'effectuer que dans le cadre d'un accord écrit conclu avec le sous-traitant ultérieur, « *imposant à ce dernier les mêmes obligations que celles qui incombent à l'importateur de données* ». **Vis-à-vis des personnes concernées, l'exportateur de données reste le garant de l'activité de traitement** dans la mesure où cette dernière doit être effectuée « *conformément à la clause 11 par un sous-traitant ultérieur offrant au moins le même niveau de protection des données à caractère personnel et des droits de la personne concernée que l'importateur de données* ».

Décision 2010/87/CE de la Commission du 5 février 2010 relatives aux clauses contractuelles types pour le transfert de données à caractère personnel vers des sous-traitants établis dans des pays tiers en vertu de la directive 95/46/CE du Parlement européen et du Conseil, J.O.U.E L. 39 du 12 février 2010, p. 5 et s.

Publication de la loi « Jeux en ligne »

La loi ouvrant à la concurrence et à la régulation du secteur des jeux d'argent et de hasard en ligne a été promulguée. Cette ouverture – partielle - est conditionnée au respect de certains enjeux : l'ordre public, la sécurité publique et la protection de la santé et des mineurs (art. 3). D'autre part, « *la politique de l'État en matière de jeux d'argent et de hasard a pour objet de limiter et d'encadrer l'offre et la consommation de jeux et d'en contrôler l'exploitation afin de :*
(…)
2° Assurer l'intégrité, la fiabilité et la transparence des opérations de jeu ; (...) »

Le déploiement des jeux en ligne ne peut donc se départir d'une analyse en termes de sécurité des systèmes d'information, à destination des opérateurs souhaitant être agréés auprès de l'ARJEL (Autorité de régulation des jeux en ligne). Cette autorité administrative indépendante veille au respect des objectifs de la politique des jeux et des paris en ligne soumis à agrément, exerce la surveillance des opérations de jeux ou de paris en ligne et participe à la lutte contre les sites illégaux (art. 34-I).

Elle fixe notamment les caractéristiques techniques des plateformes et des logiciels de jeux et de paris en ligne des opérateurs soumis au régime d'agrément et a prévu un cahier des charges très strict à destination de ces derniers. Le cahier des charges prévoit ainsi un certain nombre de garanties : protection des personnes vulnérables et prévention des comportements addictifs, transparence de leurs activités et solidité financière, régularité de leurs opérations de jeux, fiabilité et traçabilité des données de jeu (arrêté du 17 mai 2010).

Elle dispose également d'une échelle de sanctions (avertissement, réduction de l'agrément, suspension, retrait ou sanction pécuniaire) en cas de manquement des opérateurs agréés à leurs obligations et assure la lutte contre les sites illégaux de jeux d'argent (art. 56 et s. de la loi).

Enfin, on peut noter que contrairement à bon nombre de lois, les décrets et arrêtés d'application ont tous été publiés en l'espace de deux semaines… Coupe du monde oblige !

Loi n°2010-476 du 12 mai 2010 relative à l'ouverture à la concurrence et à la régulation du secteur des jeux d'argent et de hasard en ligne, J.O. du 13 mai 2010, p. 8881.

Décret n°2010-481 du 12 mai 2010, J.O. du 13 mai 2010, p.8927.

Décret n°2010-482 du 12 mai 2010, J.O du 13 mai 2010, p.8930.

Décret n°2010-483 du 12 mai 2010, J.O. du 15 mai 2010, p. 8932.

Décret n°2010-494 du 14 mai 2010, J.O. du 15 mai 2010, p. 9051.

Décret n° 2010-495 du 14 mai 2010, J.O du 15 mai 2010, p. 9052.

Décret n° 2010-498 du 17 mai 2010, J.O. du 18 mai 2010, p. 9164.

Arrêté du 17 mai 2010 portant approbation du cahier des charges applicable aux opérateurs de jeux en ligne, J.O du 18 mai 2010 p. 9165.

Décret n° 2010-518 du 19 mai 2010, J.O du 20 mai 2010, p. 9295.

Focus :

L'adresse IP et le Droit

Bien que l'adresse IP présente un caractère technique, elle revêt également une importance considérable dans le domaine juridique. En effet, depuis quelques années, le débat sur la qualification de l'adresse IP, à savoir s'il s'agit ou non d'une « donnée à caractère personnel » (DCP), est ouvert et fait l'objet de nombreuses décisions jurisprudentielles.
Afin de pouvoir appréhender avec précision les dérives commises sur Internet, il est nécessaire de connaître le statut juridique de l'adresse IP (I), son rôle dans la lutte contre la cybercriminalité (II) et, enfin, la solution législative envisagée à l'heure actuelle (III).

I. Statut juridique de l'adresse IP

A. Définitions

La notion de donnée à caractère personnel est née avec la directive européenne du 24 octobre 1995 (JO n° L. 281 du 23/11/1995 p. 0031 - 0050), remplaçant la notion « d'information nominative » instituée par la loi Informatique et Libertés du 6 janvier 1978 (JORF du 7 janvier 1978 page 227). Suite à la transposition de cette directive, par la loi du 6 août 2004 (JORF n°182 du 7 août 2004 page 14063), l'article 2 de la loi Informatique et Libertés définit une DCP comme étant « toute information relative à une personne physique identifiée ou qui peut être identifiée, directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments qui lui sont propres». Notons que la collecte et le traitement des DCP sont encadrés par la loi et contrôlés par la Commission Nationale Informatique et Libertés (CNIL), qui doit être sollicitée, préalablement à la mise en œuvre du traitement, pour faire part de son avis.

Une adresse IP (Internet Protocol) correspond au numéro permettant d'identifier chaque ordinateur connecté à Internet ou, plus généralement, l'interface avec le réseau de tout matériel informatique (routeur, imprimante) connecté à un réseau informatique utilisant l'Internet Protocol. Ces adresses IP permettent aux ordinateurs de communiquer entre eux, en leur fournissant à chacun une adresse unique utilisée pour échanger des données. Le protocole IP dans sa version 4 se présente sous la forme d'une série de quatre nombres allant chacun de 0 à 255 (soit un octet) et séparés par des points. Le nombre théorique maximal d'adresses était donc de près de 4,3 milliards. Plusieurs techniques ont été utilisées permettant une gestion parcimonieuse des adresses disponibles (réseaux internes ne possédant que quelques IP externes connectées à l'internet, etc.) et notamment le recours à des adresses dites « dynamiques », allouées par chaque fournisseur d'accès à l'internet à ses clients pour un temps limité à partir d'un pool commun, ce qui leur assurait, au moins vis-à-vis de l'extérieur, un relatif anonymat.

Pourtant, le nombre d'adresses est vite devenu trop faible au regard du nombre d'ordinateurs ou « d'objets communiquants » appelés à recevoir une adresse IP dans les années à venir.
Une nouvelle version du protocole IP a donc vu le jour, appelée IPv6 (constituée de 16 octets, elle permet plus de 667 millions de milliards d'adresses par millimètre carré de surface terrestre). Contrairement à l'adresse IPv4, l'IPv6 permet d'attribuer une adresse IP fixe à presque tous les dispositifs connectés à Internet, c'est-à-dire qu'à chaque connexion, l'internaute dispose d'une même adresse IP, ce qui le rend beaucoup plus facilement identifiable vis-à-vis de l'extérieur qu'avec l'IPv4.

D'autant plus qu'une autre différence existe : l'IPv4 était allouée par le fournisseur d'accès à l'internet et dépendait donc de l'abonnement souscrit. Or l'IPv6, elle, pourra dans certain cas incorporer l'adresse MAC (Multimedia Access Control) unique attribuée au composant réseau et donc indiquer directement le matériel utilisé pour la connexion.

Formations - Conférences :

COMUNDI, Cybersurveillance du salarié, cyberprotection de l'employeur, F. Coupez, 29 et 30 juin 2010, Paris.

Soph Conf 2010, Gestion des identités et sécurisation des services web : réalités & perspectives, Authentification et éléments de droit, P. Agosti, 30 juin 2010, Sophia Antipolis.

Soph Conf 2010, Audit juridique d'un logiciel libre : l'exemple de l'IPRA, P. Agosti, 1er juillet 2010, Sophia Antipolis.

Centre de Formation à la Sécurité des Systèmes d'Information, stage cryptologie : droit et réglementation, F Coupez, 20 septembre 2010, Paris.

Salon e-Commerce 2010, Réseaux sociaux et "social commerce" : contraintes juridiques et cadre légal, E. A. Caprioli et F. Coupez, 22 septembre 2010, Paris.

Conference on Control and Fault-Tolerant Sytems (SysTol'10) : E .A Caprioli, 6 au 8 octobre 2010, Nice.

Il paraît toutefois difficile, en superposant ces définitions, de savoir si l'adresse IP constitue une information permettant l'identification de l'internaute, et donc une DCP. Sa qualification juridique revêt pourtant une importance considérable, puisque si elle constitue une DCP, alors elle sera soumise aux dispositions de la loi de 1978 et sa collecte et son traitement devront faire l'objet de formalités déclaratives préalables auprès de la CNIL, cette dernière disposant en effet d'un contrôle à priori sur tous les traitements de DCP.

B. Qualification juridique de l'adresse IP

Dès l'origine, le Groupe de travail des autorités européennes de protection des données (aussi appelé « Groupe de l'Article 29 » ou « G29 ») ainsi que la CNIL ont considéré que l'adresse IP devait être considérée comme une DCP, au même titre qu'un numéro de téléphone ou la plaque minéralogique d'un véhicule (B. Poidevin, V. Gelles, *L'adresse IP : une donnée à caractère personnel ? Une question discutée par la jurisprudence*, 2009, disponible sur legalbiznext.com). Dans un avis du 20 juin 2007, le G29 a considéré que l'information qui permet l'identification indirecte d'une personne peut être qualifiée de DCP compte tenu des moyens mis en œuvre, par le responsable du traitement, pour identifier ladite personne. Le G29 a également estimé que la finalité des traitements mis en œuvre par les organismes de protection professionnelle, ainsi que les moyens qu'ils utilisent, permettent une possible identification du hacker.

Le point de vue de la jurisprudence nationale sur cette question est plus nuancé.
Ainsi, dans deux décisions de 2007 (CA Paris, 27 avril 2007, n° 06/02334 ; CA Paris, 15 mai 2007, n° 06/01954), la Cour d'appel de Paris a considéré que les adresses IP collectées à l'occasion de la recherche et de la constatation des actes de contrefaçon sur Internet ne permettent pas d'identifier, même indirectement, des personnes physiques et que, dès lors, elles ne constituent pas des DCP (A. Diehl, *L'adresse IP est-elle une donnée personnelle ?*, La lettre professionnelle « Recherche et Référencement », mars 2008). En effet, l'adresse IP n'aboutit à l'identification d'une personne que par l'intervention de la police ou de la gendarmerie dans le cadre d'une procédure judiciaire. A ce titre, les juges précisent, dans l'arrêt du 27 avril, que « l'adresse IP ne permet pas d'identifier le ou les personnes qui ont utilisé l'ordinateur », ajoutant, le 15 mai, « que cette série de chiffres ne constitue en rien une donnée indirectement nominative relative à la personne dans la mesure où elle ne se rapporte qu'à une machine, et non à l'individu qui utilise l'ordinateur pour se livrer à la contrefaçon ». La Cour d'appel ayant considéré, dans ces deux arrêts, que l'adresse IP ne constituait pas une DCP, la collecte et le traitement des adresses IP pouvaient donc se faire sans autorisation préalable de la CNIL. Dans une autre affaire, en 2008 (CA Paris, Ch. Corr., 29 janvier 2008), la même Cour n'a pas manqué de rappeler que l'adresse IP se rapporte à une machine et ne permet donc – selon elle – d'identifier qu'un ordinateur.

Par la suite, la jurisprudence a fait l'objet d'une évolution considérable dans un sens plus conforme à la réalité technique puisque, dans deux décisions de la Cour d'appel de Rennes (CA Rennes, 22 mai 2008, n° 08/868 ; CA Rennes, 23 juin 2008, n° 1062/08), les juges ont qualifié l'adresse IP de DCP, déclarant que l'adresse IP acquiert un caractère nominatif « par le simple rapprochement de la base des abonnés, détenue par le fournisseur d'accès Internet ». En conséquence, toute collecte et tout traitement d'adresses IP doivent désormais avoir faire l'objet des formalités prévues à la loi de 1978.

Un revirement de jurisprudence a pourtant eu lieu début 2009 (Cass. Crim., 13 janv. 2009, n° 08-84.088), dans une affaire où le prévenu contestait la conformité de la collecte de son adresse IP effectuée par un agent assermenté mandaté par la Sacem : la Cour a considéré qu'un tel traitement n'avait pas été réalisé de manière automatisée, et qu'il ne tombait donc pas dans le champ d'application de la loi de 1978. Ainsi, bien que la Cour ne se soit pas prononcée de manière explicite sur la nature juridique de l'adresse IP, elle semble toutefois partager le point de vue de ceux qui considèrent que l'adresse IP n'est pas une DCP.

Quant à la jurisprudence communautaire, elle est très claire sur la question et rejoint la doctrine de la CNIL et du G29. En effet, dans l'affaire Promusicae (CJUE, 29 janv. 2008, Aff. n° 275/06), la CJUE a dû se prononcer sur le souhait d'une association espagnole de gestion de droits d'auteur de voir son FAI révéler l'identité et l'adresse physique de certains abonnés, dont l'adresse IP ainsi que la date et l'heure de connexion. La Cour européenne a considéré que les données de connexion constituaient des DCP, déclarant « il n'est pas contesté que la communication des noms et des adresses de certains utilisateurs implique la mise à disposition de données à caractère personnel, c'est-à-dire d'informations sur des personnes physiques identifiées ou identifiables, conformément à la définition figurant à l'article 2 de la directive 95/46 ».

II. L'adresse IP, élément indispensable dans la lutte contre la cybercriminalité

A. Loi favorisant la diffusion et la protection de la création sur Internet (HADOPI 1) et loi relative à la protection pénale de la propriété littéraire et artistique sur Internet (HADOPI 2)

La polémique sur l'adresse IP a pris de l'ampleur au moment où les lois HADOPI 1 et 2 (JO 13 juin 2009, p. 9666 et JO 29 oct. 2009, p. 18290) étaient débattues au parlement. La question de l'identification, et donc de la sanction de l'internaute auteur d'une infraction sur la toile via son adresse IP, faisait en effet l'objet de nombreuses contestations. Celles-ci étaient fondées sur la responsabilité de l'abonné en cas d'utilisation de son réseau à des fins frauduleuses par un tiers.
Pour rappel, HADOPI 1 créait la Haute Autorité pour la Diffusion des Œuvres et la Protection des droits sur Internet, chargée de recueillir, auprès des fournisseurs d'accès à Internet (FAI), les adresses IP des internautes soupçonnés de piratage. Le but était de leur envoyer des avertissements puis, si besoin, les sanctionner, selon le système de la riposte graduée. Notons que cette loi a conduit à l'introduction de l'article L. 336-2 dans le Code de la Propriété Intellectuelle (CPI) qui consacre une disposition spécifique à « l'atteinte à un droit d'auteur ou à un droit voisin occasionnée par le contenu d'un service de communication au public en ligne ». Quant à HADOPI 2, destinée à répondre à la censure des principales dispositions de HADOPI 1, elle a instauré un nouveau dispositif de sanction de l'internaute qui commet des actes de téléchargement illégal. Ce dispositif comprend une peine de suspension de connexion d'une part (qui a conduit à la modification de l'article L. 335-7 du CPI), et l'attribution au juge d'un pouvoir de sanction par le biais de l'ordonnance pénale d'autre part.

La lutte contre le téléchargement illégal se poursuit avec un décret du 5 mars 2010 (JORF n° 0056 du 7 mars 2010 p. 4680) qui est venu préciser les données personnelles que les ayants droit seront autorisés à collecter. Parmi celles-ci, sont notamment visées les adresses IP des abonnés.

Pilier de la loi HADOPI, la collecte et le traitement des adresses IP des internautes suspectés de téléchargement illégal sont actuellement soumis à l'approbation de la CNIL. Ainsi, en application de cette loi, quatre organismes représentant les ayants droit de l'industrie musicale et cinématographique (l'Alpa, la Sacem, la SCPP et la SPPF) ont demandé l'autorisation de la CNIL pour pouvoir surveiller les réseaux peer to peer et collecter des adresses IP.

B. L'adresse IP au regard du droit pénal

Il est à noter qu'un réseau Wi-Fi constitue un système de traitement automatisé de données (STAD), au même titre qu'un réseau Carte Bancaire (Trib. Cor. Paris, 25 fév. 2000, n°9821770011). De ce fait, toute intrusion à une connexion Wi-Fi sera encadrée selon les termes de l'article 323-1 du code pénal qui sanctionne « le fait d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données ». En cas de connexion dans le but de détériorer volontairement le STAD, **les conséquences**

Pour aller plus loin :

Adresse IP
http://fr.wikipedia.org/wiki/Adresse_IP

Adresse IPv4
http://fr.wikipedia.org/wiki/IPv4

Adresse IPv6
http://fr.wikipedia.org/wiki/Adresse_IPv6#Structure_des_adresses_IPv6

Adresse MAC
http://fr.wikipedia.org/wiki/Contr%C3%B4le_d%27acc%C3%A8s_au_support

Décision de la Cour fédérale allemande de Karlsruhe du 11 mai 2009 : **peine d'amende de 100 €** au motif que le choix du mot de passe du protocole de sécurité Wi-Fi à défaut d'être « *suffisamment long, sûr et personnel* » **ne permettait pas de protéger son accès Wi-fi**.
http://www.spiegel.de/netzwelt/netzpolitik/0,1518,694452,00.html

sont plus importantes, les peines encourues étant alourdies (art. 323-2 et 323-3 du code pénal).

C'est à ce moment précis que l'adresse IP intervient, puisque la collecte de cette dernière est susceptible de déterminer l'auteur, responsable de l'accès ou du maintien frauduleux sur le système. Cependant, une difficulté survient : l'adresse IP permet d'identifier, dans sa version 4, le titulaire de l'abonnement auprès du FAI qui a attribué l'IP, et non l'utilisateur réel au moment de la connexion. A ce titre, il est important de rappeler qu'il existe un nombre considérable de personnes qui sécurisent mal leur réseau Wi-Fi, ou encore qu'il peut parfois y avoir confusions entre les adresses IP détectées sur les réseaux et le vrai auteur de l'acte de contrefaçon, qui a pu, lui, utiliser une adresse IP d'emprunt ou tout simplement techniquement contrefaite. A titre d'exemple, un habitant niortais, accusé d'avoir usurpé l'identité d'une femme, a été repéré grâce à son adresse IP. Or, il s'est avéré que le coupable n'était autre que le voisin qui avait piraté sa connexion Wi-Fi non sécurisée. Cette affaire a mis en évidence la fragilité de l'adresse IP comme preuve dans l'identification d'un suspect, relançant ainsi le débat du système de la riposte graduée (S. Caruana, *Une connexion Wi-Fi non sécurisée mène en garde à vue*, Brève, 2010).

Néanmoins, il convient de noter que les lois HADOPI prennent en compte cette relative incertitude : comme l'internaute téléchargeant en fraude les contenus protégés ne peut être identifié avec une absolue certitude à partir de l'IP qu'il utilise, **le législateur a décidé de rendre le titulaire de l'abonnement (et donc de l'IP) responsable des agissements effectués à partir de sa connexion, en lui imposant de sécuriser son accès** (sous peine d'une amende de 1 500 euros et d'une éventuelle coupure de son accès – décret à paraître).

Par ailleurs, notons qu'une intrusion à un système Wi-Fi, pour être sanctionnée conformément au droit pénal, doit comporter un élément matériel et un élément intentionnel (art. 121-3 du code pénal). Or, l'adresse IP ne permettant pas de déterminer avec exactitude la véritable personne auteur de l'infraction, les éléments matériels et intentionnels seront difficilement imputables à la personne titulaire de l'adresse IP, car cette dernière peut avoir été victime d'usurpation de son adresse IP.

C. Le projet de loi d'Orientation et de Programmation pour la Performance de la Sécurité Intérieure (LOPPSI II)

La LOPPSI II prévoit, en son article 2, une nouvelle incrimination qu'est le délit d'usurpation d'identité numérique. Ce délit punit d'un an d'emprisonnement le fait d'utiliser, sur un réseau de communication électronique, l'identité d'un tiers ou des données qui lui sont personnelles, sans autorisation et dans un but frauduleux, notamment en vue de porter atteinte à son honneur ou à sa réputation. Par ailleurs, concernant la lutte contre la pédo-pornographie, une liste noire de sites serait créée, portant sur les adresses Internet (a priori les adresses IP) et il incomberait aux FAI une obligation de filtrage des adresses IP désignées par arrêté du ministre de l'intérieur. Les FAI devront bloquer toute tentative de connexion vers lesdits sites. Pour ce faire, ils adresseront une commande à leurs routeurs pour les reconfigurer, de manière à ce que toute demande d'accès à une des adresses IP suspectes ne soit plus relayée directement au serveur demandé par l'utilisateur, mais soit désormais routée vers la plateforme de filtrage. En conséquence, dès lors qu'un abonné demande à accéder à une ressource hébergée sur un site dont l'adresse IP a été associée par un FAI à celui d'une URL fichée par la police, la requête est redirigée par les routeurs du FAI vers la plateforme de filtrage qui interrompt la communication si la ressource correspondante est dans la liste noire (M.A. Boutoleau, *Projet de loi Loppsi 2 sur Internet : Filtrage, fichage epiratage à tous les étages*, Acrimed, janv. 2010).

Ainsi, l'adresse IP représente un élément incontournable de la lutte contre la cybercriminalité.

III. L'adresse IP : une réponse législative sur la qualification de « donnée personnelle » ?

Une proposition de loi tendant à mieux garantir le droit à la vie privée à l'heure du numérique a été adoptée à l'unanimité, par le Sénat, le 23 mars 2010. Ce texte, qui fait directement référence aux récents débats sur les lois HADOPI dont le but était de gérer en grand nombre les adresses IP des internautes, se propose notamment de faire officiellement de l'adresse IP une DCP, conformément à la doctrine de la CNIL et du G29, et impose la transparence dans le traitement des informations personnelles.

Alors que certains tribunaux refusaient d'accorder la qualité de donnée personnelle à l'adresse IP, les sénateurs Y. Détraigne et A.M. Escoffier avaient « acquis la conviction que l'adresse IP constituait un moyen d'identifier un internaute, au même titre qu'une adresse postale ou un numéro de téléphone par exemple », d'où l'intérêt de la protéger. Ce projet de loi propose donc de modifier l'article 2 de la loi de 1978 qui viserait désormais « tout numéro identifiant le titulaire d'un accès à des services de communication au public ».

Les rapports qu'entretiennent adresse IP et droit apparaissent donc complexes et surtout évolutifs, chacun (jurisprudence, législateur, doctrine) apportant sa pierre à un édifice qui pourtant ne semblait pas si difficile que cela à construire à l'origine. La raison du débat est sans doute à trouver du côté de la protection du droit d'auteur, gênée pendant longtemps par les formalismes de la loi de 1978, qui a conduit les tribunaux à une interprétation permettant de réprimer les contrefaçons constatées en dépit de preuve qui auraient été illégales s'ils avaient considéré l'adresse IP comme une DCP. Depuis les lois Hadopi, et avec la publication attendue de l'autorisation de la CNIL pour la collecte automatisée des adresses IP des pirates téléchargeurs, le débat devrait cesser et consacrer l'interprétation logique partagée au niveau européen : l'adresse IP est une DCP.

Reste que, comme toute DCP (nom, numéro de plaque minéralogique, etc.), celle-ci peut être usurpée pour commettre notamment des délits. L'adresse IP, si elle est une DCP, n'en est surtout pas pour autant une preuve fiable d'identité de l'utilisateur !

Jurisprudence :

Dérives financières et temporelles sanctionnées par les Juges du fond : les appports du TGI de Niort du 14 décembre 2009

Le tribunal de grande instance de Niort dans un jugement rendu le 14 décembre 2009, a envoyé un signal fort aux sociétés de services informatiques prêtes à tout pour remporter un appel d'offre.

En l'espèce, la MAIF souhaitait mettre en place un système de Gestion de la Relation avec ses Sociétaires (GRS) basé sur le progiciel Siebel. Elle décide de lancer un appel d'offres destiné à faire jouer la concurrence à l'issue duquel la Société IBM est retenue. Le donneur d'ordre commande alors une étude préparatoire afin de parfaire l'analyse de ses besoins et de son environnement. A la suite de cela, un contrat d'intégration est conclu entre la MAIF et IBM par lequel cette dernière s'engageait à fournir **sur la base d'une obligation de résultat**, une solution intégrée conforme au périmètre fonctionnel et technique convenu entre les parties, en respectant le calendrier impératif fixé et pour le prix forfaitaire ferme et définitif de 7 302 822 euros HT. Or, dès le mois de février 2005, la MAIF constate un retard sur le calendrier fixé initialement entre les parties. Au mois de septembre 2005, elle demande alors par voie de lettre recommandée un dédommagement financier suite aux retards accumulés ainsi qu'un plan d'action afin d'arrêter leurs accumulations. Les deux parties s'entendent

finalement sur un règlement à l'amiable consistant au report du pilote initialement prévu pour avril 2006 à début 2007 et en une majoration de 3,5 millions d'euros de la charge financière. La signature de ce règlement à l'amiable n'a finalement pas eu lieu car IBM a constaté que le projet n'était pas « *techniquement réalisable dans les conditions initialement envisagées* ». Un nouveau protocole d'accord est alors signé le 22 décembre 2005 à l'initiative d'IBM. Toutefois, malgré la signature de ce protocole, les relations entre les parties se détériorent, la MAIF reprochant à IBM le manque de visibilité du scénario alternatif proposé. En juin 2006, la MAIF finit par décliner l'offre de 15 millions d'euros proposée par IBM qu'elle juge exorbitante au regard du prix forfaitaire initialement prévu. IBM demande alors le règlement des factures impayées mais la MAIF refuse. IBM saisit alors le tribunal aux fins d'obtenir le remboursement des factures impayées ainsi que le versement des dommages et intérêts pour rupture abusive et unilatérale de leur contrat. La MAIF a, de son côté, formé une demande reconventionnelle en nullité du contrat informatique pour vice du consentement (I) et en réparation du préjudice subi (II).

I. La nullité du contrat de prestation informatique pour vice du consentement

La MAIF reproche à la SSI d'avoir sous-évalué le calendrier et sous-estimé le budget nécessaire dans le seul but de remporter l'appel d'offres. En effet, elle estime qu'IBM s'était engagée à réaliser le projet dans un certain délai et pour un certain prix alors qu'elle savait pertinemment qu'elle ne tiendrait pas ses engagements. Pour la mutuelle, IBM n'a pas communiqué tous les éléments qu'elle aurait dû donner… pour informer son cocontractant de la réalité du périmètre du projet, de son coût et de son calendrier. La MAIF considère que le comportement d'IBM est représentatif d'une réticence dolosive conformément à l'article 1116 du Code civil.

En l'espèce, non seulement la société informatique a fait croire à la MAIF qu'elle respecterait le délai et le prix initialement convenu mais elle a également gardé le silence sur le délai et le prix réel du projet alors qu'elle en avait connaissance avant la signature du contrat d'intégration. Or, le délai et le prix étaient des éléments déterminants du consentement de la MAIF.

Les juges niortais ont retenu cette analyse en affirmant qu' « *en gardant le silence sur le risque « fort », « élevé », encouru quant à la satisfaction de conditions définies au contrat comme déterminantes (forfait, planning), et généré de son fait par la violation des normes et des règles de l'art, - risque qu'en sa qualité de professionnel hautement qualifié il ne pouvait ignorer, et dont, au demeurant il n'a jamais prétendu l'avoir méconnu, se contentant de faire valoir que la MAIF aurait par les protocoles ultérieurs renoncé au planning et au forfait - le professionnel hautement qualifié qu'est IBM…a obtenu de la MAIF une adhésion viciée quant aux dits éléments…et a ainsi caractérisé une réticence dolosive, qui affecte la validité du contrat* ».

Le consentement de la MAIF ayant été vicié, le tribunal de grande instance prononce la nullité du contrat d'intégration et des deux protocoles d'accord conclu entre la MAIF et IBM.

De nombreuses décisions de jurisprudence ont déjà retenu la responsabilité des sociétés informatiques ne respectant pas les délais contractuels (CA Colmar 13 avril 2006 concernant la responsabilité d'un fournisseur de progiciel intégré ayant exécuté ses prestations en retard par rapport au calendrier contractuel) ou le prix (CA Paris 28 mai 2008 concernant une dérive des coûts).

En revanche, le dol n'est, quant à lui, que très rarement retenu en matière de contrat informatique. La 1ère chambre civile de la Cour de cassation dans un arrêt rendu le 13 décembre 2005 a ainsi retenu le dol dans une affaire où l'éditeur d'un logiciel avait prétendu détenir tous les droits d'auteur sur le logiciel cédé alors qu'il s'était abstenu d'indiquer que ce logiciel était l'un des modules d'un logiciel antérieur dont deux autres personnes étaient co-auteurs.

Signaux de fumée (en direct du web…)

Cour de cassation, Chambre sociale, 9 février 2010 : l'inscription d'un site sur la liste des « favoris » de l'ordinateur ne confère aucun caractère personnel à la connexion établie par le salarié à partir du matériel informatique fourni par son employeur.
http://www.foruminternet.org/specialistes/veille-juridique/jurisprudence/cour-de-cassation-chambre-sociale-9-fevrier-2010-3014.html

TGI de Nanterre, 25 mars 2010 : proposer un lien profond vers le site de l'éditeur d'un logiciel pour le télécharger ne constitue pas un acte de contrefaçon.
http://legalis.net/jurisprudence-decision.php3?id_article=2897

Décret du 31 mars 2010 : obligation (non sanctionnée) d'audit des climatisations des datacenter.
http://www.lemondeinformatique.fr/actualites/lire-l-audit-de-la-climatisation-des-datacenters-devient-obligatoire-30352.html

CA Paris, 14 avril 2010 : la commercialisation de publicités par une personne exploitant un site ne permet pas d'exclure le statut d'hébergeur dès lors que le service n'est pas en mesure d'opérer sur les contenus mis en ligne un quelconque ciblage publicitaire, la publicité étant placée sur la page d'accueil et les cadres standards.
http://legalis.net/jurisprudence-decision.php3?id_article=2904

Peu de prestataires informatiques ont été condamnés pour avoir dissimulé des informations au donneur d'ordre dans le seul but de remporter un appel d'offres. Or, dans la pratique, c'est une démarche relativement courante. En effet, nombreux sont les fournisseurs informatiques qui s'engagent dans une relation contractuelle en sous-évaluant le délai et en sous-estimant le prix dans le seul but de remporter un marché quitte à modifier par la suite le délai et le prix grâce à des protocoles d'accord ou des avenants.

II. La réparation du préjudice subi

IBM a été condamnée par le tribunal de grande instance de Niort à restituer à la MAIF les sommes versées au titre de leur relation contractuelle. Toutefois, le tribunal a refusé de prendre en compte les sommes dont la MAIF a conservé le profit, à savoir les sommes correspondant **aux livrables (chantier architecture)** et les sommes versées au titre du **contrat d'étude préalable**.

De plus, la SSI doit également verser des dommages et intérêts à la MAIF pour un montant total de 9,5 millions d'euros. Cette somme comprend notamment les **coûts relatifs à la rémunération des prestataires externes et des prestataires internes ainsi que les frais relatifs au retard du projet.**

Le tribunal estime que ne doivent pas être pris en compte dans l'évaluation du montant des dommages et intérêts, le coût de maintenance du progiciel Siebel, le coût de la formation des salariés au progiciel Siebel et enfin le coût des matériels et logiciels engagés dans le projet. En effet, il estime que « *Dès lors que la MAIF ne justifie pas avoir supporté en vain le coût de maintenance du progiciel Siebel…qu'elle a conservé après l'échec du projet, ni celui de la formation au progiciel Siebel des techniciens susceptible d'être réinvesti dans le nouveau projet d'intégration Siebel, ou celui des matériels et logiciels, réutilisables, engagés dans le projet, elle sera déboutée de sa demande d'indemnisation de ces chefs* ». Le tribunal refuse également de retenir les surcoûts relatifs au nouveau projet de Gestion de la Relation avec les Sociétaires de la MAIF. Il considère qu' « *il n'existe pas entre l'engagement d'un surcoût, pour la réalisation d'un nouveau projet, nécessairement plus moderne et performant, de relation causale adéquate avec les manœuvres dolosives d'IBM ayant déterminé le consentement de la MAIF* ».

Enfin, IBM a également été condamnée à verser la somme de 50 000 euros à la MAIF au titre de l'article 700 du Code de procédure civile.

Il convient de noter que les sommes indiquées devront être versées nonobstant le fait que le géant de l'informatique a fait appel du jugement de première instance, car les sommes ont été soumises à exécution provisoire.

Cette décision est exemplaire tant au niveau du montant de la condamnation qu'à celui de l'évaluation du préjudice. En effet, chaque poste d'indemnisation a été examiné de manière précise par le tribunal. Les juges ont essayé d'indemniser au mieux le préjudice subi. **Ainsi, les magistrats ne refusent pas d'allouer des dommages et intérêts conséquents. Encore faut-il que les demandes soient justifiées.**

En résumé, lorsqu'un projet informatique connait d'importantes dérives tant financières que temporelles, mieux vaut pour le prestataire qu'il traite le problème dès qu'il en prend conscience plutôt que d'avancer en comptant sur le comportement passif de son cocontractant. La période budgétaire n'est plus à cette indolence contractuelle.

Vie du cabinet :

Le Cabinet recherche des stagiaires pour chacune des entités à compter du mois de septembre pour des périodes allant de 2 mois à 6 mois :

- en cours de diplôme d'un troisième cycle de haut niveau en droit des nouvelles technologies ou d'un DJCE ;

- maîtrisant l'anglais.

Contactez le Cabinet à l'adresse suivante : contact@caprioli-avocats.com

Une réponse… à une question :

Le cabinet a sélectionné une question concernant les bases de données :

Comment puis-je protéger ma base de données (par le droit sui generis lié aux bases de données) ?

La base de données constitue une richesse indéniable pour toute entreprise (base de données clients, fournisseurs, salariés). Pour éviter que ces dernières ne soient pillées par un concurrent ou toute autre personne, la société peut agir en justice sur le fondement de la **concurrence déloyale ou du parasitisme**, de la **contrefaçon via le droit d'auteur** ou encore, et c'est l'hypothèse qui a été retenue dans la question, par le biais du droit sui generis lié aux bases de données (article L. 341-1 du CPI).

Rappelons que trois éléments conditionnent la protection des bases de données en ligne par le droit *sui generis* :

- Il doit y avoir base de données au sens de l'article L. 112-3 al. 2 du CPI : « *un recueil d'oeuvres, de données ou d'autres éléments indépendants, disposés de manière systématique ou méthodique, et individuellement accessibles* […]». Cela peut comprendre les annuaires en ligne, les compilations de données, (…) ou encore certains sites Internet ;
- Seul le producteur de la base bénéficie de la protection. Il s'agit au sens de l'article L. 341-1 du CPI de « *la personne physique ou morale qui a pris* ***l'initiative et le risque*** *des investissements correspondants* ». Il s'agit vraisemblablement de l'entreprise mais une personne physique peut également revendiquer ce statut. A ce titre, il est important d'encadrer les contrats de travail avec ses salariés ;
- Le producteur de la base doit prouver qu'il a réalisé « *un investissement financier, matériel ou humain substantiel* » (art. L 341-1 du CPI). La preuve de cet investissement pourra être établie par des factures (prestataires, licences de logiciels...) ou des contrats de travail (salaires).

En complément de cette protection, certaines mesures peuvent venir compléter cette protection :

- la mise en oeuvre de **dispositifs techniques** empêchant les extractions massives par les automates informatiques ;
- la **préconstitution de preuves** (coquilles et erreurs d'orthographe volontaires qui seraient reprises par le contrefacteur...) ;
- **la surveillance des statistiques du serveur** pour détecter les connexions irrégulières ou les aspirations (gestion des logs) ;
- la **sécurisation juridique des contrats d'exploitation** de bases de données et des contrats de travail (clause de propriété intellectuelle, etc.) ;
- le recours au **dépôt**, qui permettra de disposer d'une preuve d'antériorité.

Pour aller plus loin, *Caprioli & Associés, Le régime juridique des bases de données, www.caprioli-avocats.com*

Cette rubrique est votre rubrique. Vous pourrez poser votre question à l'adresse 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, n'hésitez pas à nous contacter à l'adresse suivante : contact@caprioli-avocats.com.

Toute demande de désinscription à la présente Newsletter peut être effectuée à l'adresse suivante : contact@caprioli-avocats.com.