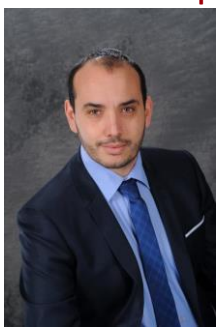
L'édito de la TiPi

Ode au Numérique



Contracter via l'Internet, poster un twit
Consulter mon compte, envoyer un courrier électronique :
Toutes ces actions et d'autres encore inédites
Relèvent désormais de notre quotidien numérique.

Mais comment prospérer sans confiance ?
Sans certitude sur l'identité de mon interlocuteur,
La date ou l'intégrité de ma correspondance,
Comment ne pas avoir peur ?

Législateurs communautaire et nationaux
Se sont saisis de cette question,
Offrant un cadre juridique aux réseaux,
Dotant de règles la dématérialisation.

Les débuts de cette révolution furent difficiles.
Les usages restaient anecdotiques,
Malgré la réforme du Code civil.
Qui aurait parié sur l'écrit électronique ?

Les Cassandre avaient tort.
L'Internet subit de nombreuses mues
Mais se déploie toujours et encore
Dans des domaines inconnus.

Mais le doute subsiste
Sur la sécurité juridique des échanges dématérialisés.
Confrontés aux poussées consuméristes
De nombreux pans du Droit ont été modifiés.

Les commandes en ligne, les remises de contrats,
La signature ou les modalités de rétractation
Avaient jeté les patriciens dans l'embarras.
Et il fallut bien des nuits de méditation.

Pour que d'esprits juridiques
Exultent des montages ingénieux,
D'intéressantes cinématiques,
Des contrats informatiques ambitieux.

Le Numérique est désormais partout présent,
Modifiant jusqu'à notre structure de mémoire.
L'homme nouveau se dessine méthodiquement.
Certes différent mais toujours porteur d'espoir.

Pascal AGOSTI
Avocat au Barreau de Nice
Docteur en droit

Aujourd'hui dans la TiPi :

Actualités

Renforcement de la répression contre la contrefaçon

Loi n° 2014-315 du 11 mars 2014 renforçant la lutte contre la contrefaçon, JO du 12 mars 2014 p. 5112.

La loi n° 2014-315 du 11 mars 2014, renforçant la lutte contre la contrefaçon, a pour objectif de renforcer l'arsenal législatif existant. Dans ce but, elle modifie le Code de la propriété intellectuelle, le Code des douanes, le Code de la sécurité intérieure et le Code des postes et des communications électroniques afin notamment d'améliorer le mode de calcul des dommages et intérêts alloués aux victimes, de clarifier la procédure en matière d'action en contrefaçon (notamment du fait de certaines interprétations tirées de la loi du 29 octobre 2007) et de renforcer les pouvoirs des agents des douanes.

Dans le détail, ses chapitres I à IV apportent des précisions notables concernant les règles de procédure en cas d'action en contrefaçon. Ainsi, la loi renforce le droit à l'information des victimes pour tous les « produits argués de contrefaçon » (art. 3), aligne les délais de prescription des actions en contrefaçon avec le délai prévu en droit commun de 5 ans (art. 16). Ensuite, cette loi renforce les dédommagements civils accordés aux victimes de contrefaçon, le juge pouvant prendre en considération l'ensemble des conséquences économiques négatives dans le cadre d'une action en contrefaçon (prise en compte des économies d'investissements intellectuels, matériels et promotionnels tirés de l'atteinte aux droits, etc., cf. art.2). Enfin, les chapitres III et IV de la loi modifient les dispositions relatives au droit de la preuve en matière de procédure de saisie-contrefaçon (saisine des documents se rapportant au produit contrefaisant, etc.).

La loi renforce également les pouvoirs des agents de l'administration des douanes. Le chapitre V modifie l'article L. 355-11 du Code des douanes dans le but d'élargir le pouvoir de retenue des marchandises susceptibles de porter atteinte aux droits de propriété intellectuelle (prise d'échantillons, destruction, etc.). L'article 10, modifiant l'article 67 *bis*-1, élargit à l'ensemble des marchandises contrefaites non seulement le pouvoir des agents en matière de « coups d'achat » (procédure qui consiste, pour un douanier, à procéder à l'acquisition d'une certaine quantité de produits soupçonnés de constituer des contrefaçons afin de vérifier si la contrefaçon est ou non avérée), mais également les pouvoirs des agents en matière « d'infiltration » en permettant la mise en cause d'autres catégories de personne (notamment les personnes « intéressées »). L'article 15 de la loi prévoit, quant à lui, la possibilité pour les douaniers d'avoir accès à des locaux privatifs avec l'assentiment express de l'occupant ou de son représentant, ainsi qu'aux locaux professionnels des *« prestataires de services postaux et des entreprises de fret express »* (art. 12), ces derniers ayant l'obligation de transmettre automatiquement les données relatives à l'identification des marchandises aux agents des douanes (nouvel art. 67 sexies). Ces pouvoirs s'accompagnent de garanties procédurales pour les sociétés (procès-verbal, respect de la loi de 1978 concernant le traitement de données mis en place par la douane).

Enfin, la contrefaçon de marques portant sur des marchandises dangereuses pour la santé ou la sécurité de l'homme ou de l'animal devient une circonstance aggravante, les sanctions pénales s'élevant dorénavant à 5 ans de prison et 500.000 € d'amende (L. 716-10 du Code de la propriété intellectuelle).

Le titre restaurant se dématérialise

Entré en vigueur le 2 avril 2014, le décret n° 2014-294 relatif aux conditions d'émission et de validité et à l'utilisation des titres-restaurant vient formaliser le cadre d'une dématérialisation que certains acteurs avaient déjà opérée dans le silence des anciens textes (art. 1 modifiant l'article R. 3262-1 du Code du travail).

Le décret retouche également certaines dispositions applicables aux titres-restaurant sur support papier pour lesquelles l'utilisation d'un support dématérialisé n'aurait pu être garantie (limitation des mentions obligatoires aux seuls noms et adresses de l'émetteur et de la banque garantissant le remboursement à l'établissement au profit desquels les titres peuvent être débités, caractère certain du paiement garanti par la tenue, à la charge de l'émetteur, d'un registre faisant correspondre les numéros de série des titres dématérialisés à un identifiant personnel de l'utilisateur - art. 2 -, etc.). Le décret prévoit également que le salarié, utilisant un titre dématérialisé, sera débité de la somme exacte à payer, dans la limite de 19 euros par jour (art. 6 modifiant l'art. R. 3262 du Code du travail) et, plus généralement, que cette utilisation sous forme dématérialisée permettra de rendre plus efficace les limitations du titre : pas d'utilisation les dimanches et jours fériés sauf exception, durée d'utilisation limitée dans le temps, etc.). Ces interdictions, mentionnées de façon apparente sur les titres papier, doivent faire l'objet d'une information aux salariés (art. 5).

Décret n° 2014-294 du 6 mars 2014 relatif aux conditions d'émission et de validité et à l'utilisation des titres-restaurant, JO du 7 mars 2014 p.4928.

Ce décret n'imposant aucune technologie en particulier, l'utilisation de cartes avec ou sans contact, de smartphones ou d'autres moyens techniques apparaît donc possible, même si la protection des données à caractère personnel des utilisateurs doit notamment être prise en compte dans le cadre de leur sécurisation.

Impacts de la loi sur la consommation sur le droit de l'informatique et du commerce électronique

Censurée par le Conseil constitutionnel sur les aspects relatifs à la création du registre national des crédits aux particuliers en raison de l'atteinte disproportionnée au droit au respect de la vie privée, la loi sur la consommation vient transposer en droit français la directive 2011/83/UE sur les droits des consommateurs du 25 octobre 2011.

Elle prévoit diverses dispositions majeures, dont l'action de groupe permettant un recours collectif pour certains contentieux de masse (hors domaines de la santé et de l'environnement) : une association de consommateurs agréée au niveau national peut ainsi agir en justice contre un professionnel pour un groupe de consommateurs, dans le cas de la vente de biens ou de la fourniture de services, ou dans le cas de pratiques anticoncurrentielles.

Loi n° 2014-344 du 17 mars 2014 relative à la consommation, JO du 18 mars 2014 p. 5400.

Forte de 161 articles, dont certains modifient plusieurs pans du droit de la consommation à eux seuls, la liste exhaustive de l'ensemble de ses apports pourrait remplir un numéro de TiPi à elle seule. De façon succincte, on notera notamment que la loi prévoit dorénavant :

- le renforcement de l'obligation de communication de l'information précontractuelle (caractère lisible et compréhensible des informations, amendes administratives, etc.) ;

- l'application automatique d'une décision déclarant une clause abusive à tous les contrats identiques conclus par le même professionnel avec des consommateurs ;
- l'extension du délai de rétractation à 14 jours, à l'égal de la commercialisation à distance de services financiers, avec remboursement sous 14 jours des frais perçus dont les frais de livraison (les frais de retour restant à la charge du consommateur) ;
- la prolongation du délai durant lequel les défauts de conformité sont présumés exister au moment de la délivrance (passage de 6 à 24 mois au 18 mars 2016) ;
- l'accroissement des pouvoirs de la DGCCRF (possibilité d'être un « client mystère », de demander le blocage des sites pour prévenir un dommage, de prononcer des amendes administratives, de constater certaines infractions et manquements à la loi informatique et libertés, etc.) ;
- l'encadrement des relations fournisseurs-distributeurs (communication des CGV, formalisme renforcé, etc.) ;
- l'alourdissement important du montant des amendes pénales, notamment pour fraudes économiques, qui sont pour la plupart décuplées et peuvent aller jusqu'à 10% du chiffre d'affaires moyen annuel sur 3 ans d'une entreprise dans certains cas (pratiques commerciales trompeuses ou agressives, tromperies, etc.) ;
- la possibilité pour la CNIL de constater les infractions et les manquements à la loi « Informatique et Libertés » directement en ligne ;
- pour les achats importants (montant fixé par décret), la proposition systématique d'un crédit amortissable au lieu d'un crédit renouvelable ;
- l'assouplissement des conditions de résiliation de certains contrats d'assurance ;
- l'information sur l'existence et la disponibilité des pièces détachées pour lutter contre l'obsolescence programmée ;
- la création d'un registre d'opposition au démarchage téléphonique faisant interdiction à tout professionnel de démarcher téléphoniquement un consommateur inscrit sur cette liste, sauf en cas de relations contractuelles préexistantes ;
- l'interdiction des numéros masqués en matière de démarchage téléphonique ;
- l'extension des identités géographiques protégées aux produits artisanaux et manufacturés ;
- Etc.

Référentiel de labellisation CNIL pour les Coffre Forts Numériques

La CNIL a adopté un référentiel pour la labellisation des services de coffre-fort numérique dans le prolongement de sa Recommandation du 19 septembre 2013. La candidature au label doit être déposée par l'opérateur technique et par le fournisseur du service (qui propose le service à des personnes physiques). Ce référentiel comporte vingt-deux exigences, cumulatives, concernant la démarche de conformité à la loi « Informatique et Libertés » du candidat pour l'ensemble des traitements qu'il met en œuvre, dont l'accomplissement des formalités déclaratives auprès de la CNIL et pour le service de coffre-fort numérique (intégrité, disponibilité et confidentialité des données stockées).

Label CNIL Coffre fort Numérique, disponible à l'adresse http://www.cnil.fr/linstitution/labels-cnil/coffre-fort-numerique/.

Focus

Le m-commerce saisi par le Droit

En 2013, l'ordinateur semble presque dépassé : en France, 27 millions de personnes sont équipées de Smartphones et 7,9 millions possèdent une tablette (1). Le développement d'applications est donc devenu incontournable pour bon nombre d'entreprises afin de toucher le public le plus large.

« *Les obligations d'information et de transmission des conditions contractuelles visées aux articles 19 et 25 sont satisfaites sur* ***les équipements terminaux de radiocommunication mobile*** *selon des modalités précisées par décret* ». Il s'agissait de l'article 28 de la Loi pour la confiance dans l'économie numérique du 21 juin 2004 (LCEN) (2), seule disposition spécifique à la contractualisation via téléphone mobile qui a été abrogée en 2011 (3). En l'absence, à l'heure actuelle, de règles spécifiques, **le droit commun s'applique au « m-commerce » :** Code civil, Code de la consommation, Loi Informatique et Libertés (4), LCEN, etc. Toutefois, compte tenu du format de l'outil, une attention particulière devra être portée à trois étapes de la contractualisation lors du déploiement d'une cinématique : le développement de l'application (I.), l'authentification du prospect ou du client (II.) ainsi que la mise à disposition de l'information contractuelle (III.).

I. Le développement de l'application

Compte tenu des risques élevés de perte, de vol ou de piratage, le développement d'une application impose de prendre en compte dès le départ **la question de sa sécurité et des données qu'elle est amenée à collecter**. La mise en place de telles mesures est d'autant plus importante que de nombreux Smartphones sont déverrouillés (ou « jailbreackés » concernant les appareils Apple) et présentent plus de risques de piratage.

A ce titre, certains documents, émis par des autorités en charge de la sécurité des systèmes d'information telle que l'Agence Européenne chargée de la sécurité des réseaux et de l'information (ENISA) (5) ou l'Agence nationale de la sécurité des systèmes d'information (ANSSI) (6) ont établi des guides pratiques. Sont ainsi privilégiées certaines bonnes pratiques comme la mise en place de dispositifs adéquats contre toute intrusion de tiers ou de programmes malveillants, d'un protocole de sécurisation des échanges ou encore, la déconnexion automatique du terminal lorsque l'utilisateur quitte l'application, le blocage de l'accès après plusieurs tentatives d'authentification infructueuses.

Ces mesures de sécurité devront être adaptées en fonction de la sensibilité des données à caractère personnel traitées. En effet, comme pour la contractualisation sur l'Internet, la loi Informatique et libertés s'applique et notamment l'article 34 qui impose au responsable de traitement de prendre les mesures utiles pour préserver la sécurité des données sous peine de sanctions pénales (cinq ans d'emprisonnement et de 1 500 000 euros d'amende pour les personnes morales en application de l'article 226-17 du Code pénal).

Les règles applicables aux Smartphones en matière de protection des données ont d'ailleurs été rappelées dans un avis du G29 (Groupe regroupant les CNIL européennes) publié le 14 mars 2013 (7). Outre le rappel des différentes exigences relatives à la collecte licite des données (consentement libre, spécifique et informé des utilisateurs), l'accent a été mis sur le principe de *Privacy by design,* c'est-à-dire la prise en compte de la protection des données à caractère personnel dès la conception

(1) Baromètre du Marketing Mobile 2013, Mobile Marketing Association France.
(2) Loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique ; JO du 22 juin 2004 p. 11168.
(3) Loi n°2011-525 du 17 mai 2011 de simplification et d'amélioration de la qualité du droit, JO du 18 mai 2011 p. 8537 ; Proposition d'amendement **http://www.senat.fr/amendements/commissions/2009-2010/130/Amdt_COM-249.html.**
(4) Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, JO du 7 janvier 1978 p. 227.
(5) ENISA, Smartphone Secure Development Guidelines for App Developers, du 25 novembre 2011 : http://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-applications/smartphone-security-1/smartphone-secure-development-guidelines
(6) ANSSI, Recommandations de sécurité relatives aux ordiphones, le 19 juin 2013, N° DAT-NT-010/ANSSI/SDE/NP : http://www.ssi.gouv.fr/IMG/pdf/NP_Ordiphones_NoteTech.pdf

[…]de l'application.

La sécurisation de l'application est également l'affaire des utilisateurs de l'application. Ainsi, la mise en place de dispositions au sein des CGU peut permettre d'écarter la responsabilité de l'entreprise en cas de dommages causés par un comportement de l'utilisateur : incident occasionné sur un Smartphone déverrouillé, Smartphone ne disposant pas d'une procédure active de blocage (code PIN), etc.

Enfin, le plus grand soin devra être apporté aux documentations techniques et contractuelles concernant l'intégration des applications sur les plateformes (Google Store, AppStore…). En effet, les toolkits à destination des développeurs mettent à leur charge de nombreuses obligations en termes de développement. Il s'agira donc d'un prérequis.

II. Authentification du prospect ou du client

Il résulte des articles 1316-1 et 1316-4 du Code civil que l'identification du signataire est une condition nécessaire à la reconnaissance de l'écrit et de la signature électroniques. La contractualisation en ligne via Smartphone impose donc, comme pour tout type de contrats dématérialisés, l'authentification du client.

Plus particulièrement, certains secteurs d'activités, comme les services financiers, imposent des obligations spécifiques en matière d'identification. Ainsi, l'article L. 561-5 du Code monétaire et financier (CMF) impose d'identifier le client préalablement à l'opération « ***par des moyens adaptés*** » et de vérifier « *ces éléments d'identification* ***sur présentation de tout document écrit probant*** » (8). **Lorsque le client ou son représentant légal n'est pas physiquement présent aux fins de l'identification**, les articles L. 561-10 et R. 561-20 du CMF prévoient que l'établissement bancaire doit mettre en place une mesure de vigilance complémentaire (obtention d'une pièce justificative supplémentaire ; mise en œuvre de mesures de vérification et de certification de la copie du document officiel par un tiers indépendant, etc.).

En tout état de cause, l'utilisation des Smartphones favorisant l'envoi de documents photographiés, il est nécessaire de mettre en place un contrôle de lisibilité des justificatifs. L'entreprise devra refuser la souscription à un produit ou service dès lors que l'authentification du client ne lui semblera pas assurée, écartant, vraisemblablement, la contractualisation avec de simples prospects.

III. Mise à disposition des informations contractuelles

Plusieurs textes imposent dans le cadre de la conclusion d'un contrat électronique et donc par Smartphone la mise à disposition d'informations précontractuelles et contractuelles :

- **L'article 19 de la Loi pour la confiance dans l'économie numérique** impose d'assurer un accès facile, direct et permanent aux informations permettant d'identifier le prestataire de service.
- **L'article 1369-4 du Code civil** impose de mettre à disposition les conditions contractuelles applicables « *d'une manière qui permette leur conservation et leur reproduction* » et prévoit que l'offre doit énoncer un certain nombre d'éléments (différentes étapes à suivre, moyens techniques permettant d'identifier et de corriger les erreurs, conditions d'accès au contrat archivé, etc.).

(7) G-29, avis 02/2013, 27 mars 2013 : http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp202_en.pdf

(8) Lorsque le client est une personne physique, cette vérification s'effectue, « *par la présentation d'un document officiel en cours de validité comportant sa photographie. Les mentions à relever et conserver sont les nom, prénoms, date et lieu de naissance de la personne, ainsi que la nature, les date et lieu de délivrance du document et les nom et qualité de l'autorité ou de la personne qui a délivré le document et, le cas échéant, l'a authentifié* » (R. 561-5 du CMF).

- Le **Code de la consommation** impose de communiquer au consommateur en temps utile avant son engagement un certain nombre d'informations (identification du professionnel, conditions de l'offre contractuelle, existence ou non du droit de rétractation etc.) « *dont le caractère commercial doit apparaître sans équivoque* » et qui sont fournies de manière « *claire et compréhensible par tout moyen adapté à la technique de communication à distance utilisée* » (L. 121-18 et L. 121-20-10 - pour les services financiers - du Code de la consommation).

Ces informations devront être mises à disposition sans que le destinataire n'ait à effectuer une action particulière. Il a été reconnu que le fait que l'internaute doive agir en cliquant sur un lien hypertexte pour prendre connaissance des informations contractuelles ne permettait pas de considérer que les informations pertinentes avaient été fournies, cette méthode ne garantissant pas que le contenu de la page acceptée par l'utilisateur n'ait pas été modifié dans le temps. De plus, le lien peut également être désactivé et les informations rendues inaccessibles (9). De même, dans une affaire où le client d'un opérateur de téléphonie mobile avait été informé par SMS de la modification des conditions contractuelles et était invité à consulter le détail sur le site internet de l'opérateur, il a été considéré que cette information ne respectait pas les exigences légales qui, en matière de services de communications électroniques**, imposent une information explicite avant tout projet de modification « *et ce, dans la continuité du droit commun des contrats qui exige que le consentement du cocontractant soit éclairé quant au contenu du contrat et donc quant à la modification de ce contenu* »** (10). Si cette décision a été prise en application des dispositions spécifiques aux contrats conclus avec des opérateurs de communications électroniques, elle met en exergue, indirectement, **le fait que le recours au multi-canal est possible, pourvu que le canal choisi pour souscrire fournisse l'ensemble des informations requises.**

Le processus de contractualisation retenu devra prévoir la communication sur l'application mobile de l'ensemble des informations précontractuelles et contractuelles requises par les textes, permettre un défilement de l'ensemble de ces informations et assurer que le consommateur en a effectivement pris connaissance (case à cocher après défilement des pages par exemple couplé à une nouvelle authentification à des fins de renforcement de la manifestation du consentement). De façon complémentaire, les informations pourront être adressées par un autre moyen (enregistrement sur le Smartphone, courrier papier ou électronique, etc.). Cette solution permettra en outre de respecter l'exigence d'accessibilité des conditions durant la relation contractuelle.

De plus, **le caractère lisible des informations peut avoir un impact important pour certains contrats** comme par exemple les contrats de crédit à la consommation (11), le contrat d'assurance (12) ou encore en matière de contrat d'épargne (13). Ainsi, l'application devra être prévue de façon à ce que le choix de la police de caractère, du graphisme et de l'ergonomie ne soit pas un obstacle à la lisibilité du texte. **Les clauses importantes du contrat pourraient faire l'objet d'une page spécifique qui met en exergue les prérequis techniques importants et ce, avant le défilement des documents contractuels sous format pdf.**

(9) CJUE, 5 juillet 2012, Content Services Ltd c/ Bundesarbeitskammer (C-49/11) : http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:62011CJ0049:FR:HTML.

(10) J. proximité Antony, 12 mars 2007, M. X. c/ NRJ Mobile : Revue de Droit bancaire et financier n° 1, Janvier 2008, comm. 23.

(11) Art. R. 311-5-I du Code de la consommation : le contrat de crédit est « *rédigé en caractères dont la hauteur ne peut être inférieure à celle du corps huit. Il comporte de manière claire et lisible* ».

(12) Art. L. 112-3 alinéa 1 du Code des assurances : « *Le contrat d'assurance et les informations transmises par l'assureur au souscripteur mentionnées dans le présent code sont rédigés par écrit, en français, en caractère apparents.* […] ».

(13) Cour d'appel de Dijon, 15 janvier 2008, N° de RG: 06/01907.

Jurisprudences

ANSES : Atteinte au STAD et vol de fichiers informatiques

Dans un arrêt du 5 février 2014, la Cour d'appel de Paris a statué dans l'affaire de « l'exfiltration » de documents des serveurs de l'Agence nationale de sécurité sanitaire de l'alimentation, de l'environnement et du travail (ANSES) qui est un Opérateur d'importance vitale (OIV).

Un internaute qui, à la suite d'une recherche sur Google, avait pu accéder et télécharger des données confidentielles sur un serveur extranet de l'ANSES (dont la sécurité des paramètres d'identification était à cet instant défaillante) et avait publié un article accompagné de documents confidentiels, avait été relaxé. **La Cour d'appel a confirmé la relaxe pour accès frauduleux dans un système de traitement automatisé de données (STAD), cet accès ayant été permis par une « *défaillance technique concernant l'identification existant dans le système* ». Elle a, en revanche, condamné l'internaute à une amende de 3.000 € au motif que la découverte du contrôle d'accès signifiait qu'il avait « *conscience de son maintien irrégulier* ». De plus, le téléchargement - à des fins personnelles - de fichiers inaccessibles au public ainsi que la réalisation de copies sur différents supports à l'insu de leur propriétaire était constitutif de « *vol de fichiers informatiques* »**. Un pourvoi en cassation a été formé.

Les éléments de fait présentés en appel concernant les circonstances de cet accès expliquent que cet arrêt aille dans le sens des principes de la décision Kitetoa (*CA Paris, 30 octobre 2002*) : il y avait eu relaxe en l'absence d'éléments de nature à prouver la conscience de l'accès et du maintien irréguliers, alors que, dans cette affaire, la visualisation de certains écrans a priori explicites sur leur accès restreint, démontre cette conscience.

En revanche, en reconnaissant le « *vol de fichiers informatiques* », cette décision va à contrecourant de la jurisprudence classique selon laquelle le vol ne porte pas sur l'information elle-même mais sur l'appropriation de son support matériel (*C.Cass. crim., 20 octobre 2010*) et adopte le concept du vol-reproduction plus adapté aux infractions numériques (*TGI Clermont-Ferrand, 26 sept. 2011, Stés X. et Y. c/ Mme Rose : Comm. com. électr. 2012, comm. 36, obs. Éric A. Caprioli*).

En l'absence d'une jurisprudence plus abondante ou d'une décision de la Cour de cassation, il est encore difficile de considérer qu'il s'agit d'un principe établi.

En pratique, l'existence d'un dispositif de protection, qu'il soit technique ou informationnel est le moyen le plus simple de protéger l'accès au système d'information mais également de faire la preuve du caractère irrégulier de l'intrusion et du vol des fichiers qui pourraient en découler.

Commentaire de l'arrêt de la Cour d'appel de Paris, Pôle 4, chambre 10, du 5 février 2014 : http://www.caprioli-avocats.com/69-articles/actualites/285-caractere-frauduleux-de-l-acces-et-du-maintien-dans-un-stad-non-protege-et-vol-de-fichiers-informatiques ; CCE, Avril 2014, comm. 40, note E. A. CAPRIOLI.

Google à nouveau sur la sellette pour abus de position dominante

Google finira par connaître la procédure française sur le bout des doigts en raison des multiples contentieux diligentés à son encontre, notamment sur le fondement de pratiques anticoncurrentielles (voir TIPI, Eté et Automne 2013, Focus, *Déréférencement, position dominante : peut-on dompter les moteurs de recherche ?*).

L'affaire dont il est question porte – à nouveau – sur un éventuel abus de position dominante. Eventuel en ce que la Cour d'appel de Paris a sursis à statuer sur la caractérisation précise de celui-ci, faute d'avoir obtenu les éléments nécessaires.

La société française Bottin Cartographes commercialise des solutions de cartographie multimédia (cartes, plans et itinéraires) pouvant être intégrées dans un site Internet et se trouve en situation de concurrence directe avec la société Google Inc. qui propose gratuitement aux entreprises éditrices de sites web un service de cartographie dénommé « Google Maps API (Application Programming Interface) », une version enrichie étant également fournie moyennant paiement (« Google Maps API Premier »).

Cour d'appel de Paris, Pôle 5, chambre 4, 20 novembre 2013, Google France, Google Inc. / Bottin Cartographies.

Alors que le Tribunal de commerce de Paris a considéré que le « monopole de fait » de Google sur le marché des moteurs de recherche avait pour effet de placer la société en position dominante sur le marché connexe de la cartographie multimédia et que la vente à prix nul de « Google Maps API », constitutif d'un comportement de prédation, conduisait à l'éviction de ses concurrents, la Cour d'appel a préféré surseoir à statuer.

En effet, la Cour procède à l'examen complet des critères de nature à identifier un abus de position dominante tel que prévu à l'article 420-2 du Code de commerce :

- sur le **marché pertinent**, la Cour constate que les parties ne contestent pas l'existence d'un marché de la publicité en ligne et d'un marché de la cartographie en ligne ;
- sur la **position dominante** de Google, la Cour retient que ce dernier est en position dominante sur le marché de la publicité en ligne, lui assurant ainsi une position prééminente sur le marché de la cartographie en raison de la connexité de ceux-ci. A ce titre, la Cour rappelle que la CJUE considère que le pouvoir de marché détenu sur le marché dominé s'étend aussi au marché non dominé en raison de circonstances particulières telles que la position prééminente ;
- sur l'**abus**, la Cour estime ne pas disposer des éléments nécessaires pour statuer dès lors que Google s'est retranché derrière le secret des affaires pour ne produire aucun élément comptable, à l'exception d'une expertise excluant la pratique de prédation. La Cour considère que cette étude, réalisée par un tiers, sur demande de Google, ne peut être probante à elle-seule.

Aussi, la Cour a choisi de saisir l'Autorité de la concurrence, sur le fondement de l'article L. 462-3 du Code de commerce, lui demandant de rendre un avis sur le caractère anticoncurrentiel de la pratique alléguée, en procédant à « *l'examen du marché pertinent, du marché affecté, de la position de la société Google sur ce marché et de la consitution de l'abus de prédation* ».

Si l'Autorité de concurrence a eu l'occasion de se pencher sur les activités de Google à différentes reprises (*affaire Navx, décisions n° 10-MC-01 du 30 juin 2010 et n°10-D-30 du 28 octobre 2010 ; Avis n° 10-A-29 du 14 décembre 2010 sur le fonctionnement concurrentiel de la publicité en ligne*), elle s'est déjà heurtée au manque de transparence de celui-ci, relevant que « *Google n'a pas donné d'éléments chiffrés permettant d'apprécier sa position sur un tel marché* » (*décision n° 10-MC-01 du 30 juin 2010, cf. point 132*).

Cependant, Google a présenté jusqu'à présent des engagements de nature à convaincre, tant l'Autorité de concurrence française que la Commission européenne (Communiqué de presse du 5 février 2014), de sa volonté de remédier à la situation.

A noter, toutefois, que Google est toujours visé par un certain nombre de procédures sur le fondement de pratiques anticoncurrentielles, dont une lancée par Eurocities, un fournisseur de cartographie, devant l'autorité de concurrence fédérale allemande (Bundeskartellamt).

Affaires à suivre…

Vie du Cabinet :

Le Cabinet Caprioli & Associés tient à féliciter Mlle Marion SOLER et Meriem LADJALI, participantes au Concours National de Plaidoierie en Propriété Intellectuelle, organisé cette année à Montpellier et pour lequel ces dernières ont atteint les demi-finales (www.cn2pi.fr).

Deux nouveaux ouvrages seront bientôt disponibles en librairie :

- Eric A.CAPRIOLI, *Signature électronique et dématérialisation*, LexisNexis, 2014 ;
- Cabinet Caprioli & Associés, *La Banque en ligne et le Droit*, Essentiels de la banque et de la finance, RB édition, 2014.

Entretien avec :

Gérard GALLER

Quelles sont les ambitions et le conteu du futur règlement eIDAS ?

L'ambition du futur règlement eIDAS est de doter les citoyens, administrations publiques et sociétés privées de l'Union européenne des «outils» essentiels pour l'exécution de manière sûre et simple des transactions électroniques. Le règlement n'impose jamais l'utilisation de ces outils.
Le règlement se substituera à la directive sur les signatures électroniques de 1999. En ce qui concerne la signature électronique, eIDAS propose une simple évolution pour améliorer le cadre juridique de la directive en le clarifiant et en permettant de référencer des normes pour favoriser l'interopérabilité des signatures. Par exemple le règlement instaure une définition unique de la signature «qualifiée» (c'est-à-dire une signature électronique fiable réputée équivalente à une signature manuscrite) qui sera d'emblée applicable dans tous les pays de l'Union. **Le règlement reconnaît aussi qu'une signature serveur (ou signature mobile ou signature en nuage) peut être «qualifiée».**

Outre la signature, eIDAS définit au niveau européen des services de confiance qui n'ont aujourd'hui de valeur juridique qu'au niveau national: l'horodatage électronique, les services d'envoi recommandé électronique et les services de certificats pour l'authentification de sites web et les cachets électroniques (l'équivalent électronique du timbre caoutchouc – un nouveau concept dans l'ordre juridique de presque tous les Etats membres de l'UE). eIDAS instaure aussi le **principe d'équivalence entre documents papier et électroniques**. Le règlement définit des exigences essentielles pour la supervision étatique des prestataires de services de confiance. Finalement, eIDAS instaure la reconnaissance mutuelle entre Etats membres de l'Union de certains moyens d'identification des personnes physiques et morales.

Où en est-on de son adoption ?

Le 4 juin 2012, la Commission européenne adopta la proposition de règlement. Cet événement démarra la *procédure législative ordinaire* (anciennement appelée *codécision*) prévue à l'article 289 du Traité de Lisbonne qui requiert une décision conjointe du Parlement européen et du Conseil pour adopter une proposition de la Commission.

Le 25 février 2014, en accord avec la Commission, le Parlement et le Conseil ont trouvé un compromis informel pour un texte. Le compromis ne modifie que marginalement la substance du texte originel de la Commission mais en améliore la clarté. Le Parlement réuni en assemblée plénière le 4 avril 2014 a voté en faveur du compromis. **Le texte est actuellement en cours de révision linguistique et juridique**. Cette révision qui ne modifie pas la substance du texte a habituellement lieu avant le vote mais pour des questions de calendrier, le Parlement sortant s'est prononcé avant les corrections. Le texte révisé sera soumis à l'approbation du prochain Parlement et ensuite du Conseil. Le règlement pourra alors être publié au Journal officiel de l'Union européenne vraisemblablement **vers la fin de l'été ou au début de l'automne 2014.**

Biographie

Gérard Galler est ingénieur électricien de l'Université Libre de Bruxelles et titulaire d'un maîtrise en intelligence artificielle de l'Essex University.

Il débuta sa carrière dans le secteur privé en gérant des projets de conception de logiciels tels que la télémétrie du lanceur Ariane V, le contrôle de laminoirs, les paiements électroniques sur Internet ou la gestion optimisée de la circulation routière.

Depuis 1998, il est fonctionnaire à la Commission européenne. Il y a géré le financement par le programme-cadre de recherche de l'UE d'une vingtaine de projets sur la carte à puce. Il a conçu «*eEurope Smartcards*», une initiative politique au début des années 2000 pour favoriser le déploiement paneuropéen des cartes à puce. De 2003 à 2006, il a été conseiller scientifique des Délégations de l'UE en Géorgie et Arménie, où il a aussi géré les programmes *EuropeAid* d'aide au développement. A la Direction générale CONNECT, il est en charge depuis 2008, de la directive sur les signatures électroniques et il est un co-auteur de la proposition de «*règlement sur l'identification électronique et des services de confiance pour les transactions électroniques dans le marché unique (eIDAS)*».

Quand le Règlement entrera-t-il en vigueur ?

Le règlement eIDAS entrera *en vigueur* vingt jours après publication. Cependant, il ne sera *applicable* qu'à **la mi-2016**, à l'exception de certaines clauses. Il abrogera alors la directive. Les dispositions permettant à la Commission d'adopter la législation secondaire du règlement seront applicables dès son entrée en vigueur. Il est prévu que la reconnaissance mutuelle des moyens d'identification électronique deviendra obligatoire pour les Etats membres à la **mi-2018** (elle sera optionnelle dès la mi-2015).

Où en sont les actes délégués et les actes d'exécution ?

En vertu de l'article 290 du Traité, eIDAS confère à la Commission une délégation de pouvoir, sous contrôle du Parlement et du Conseil, pour adopter un *acte délégué* pour compléter «certains éléments non essentiels», en l'occurrence les exigences sur les organismes ayant le pouvoir de certifier la conformité des dispositifs qualifiés de création de signature électronique. Par l'article 291 du Traité, le règlement confère à la Commission une compétence d'exécution pour la mise en œuvre du règlement en lui donnant le pouvoir d'adopter sous contrôle des Etats membres, des *actes d'exécution*. Une trentaine d'actes sont prévus, la plupart sont optionnels.
La majorité des actes permettra si nécessaire, de désigner des normes dont le respect entrainera une présomption de conformité aux exigences du règlement. Par exemple, un dispositif de signature conforme à une certaine norme de sécurité sera réputé remplir les exigences d'un dispositif «qualifié» tel que détaillé dans le règlement. D'autres actes consisteront à définir si nécessaires des procédures applicables aux autorités publiques. Les quelques actes obligatoires du règlement serviront à définir un cadre d'interopérabilité des moyens d'identification, **un label pour les prestataires de services qualifiés, le format de la «liste de confiance» – une espèce de répertoire des prestataires qualifiés ou les formats de signature** que les administrations publiques devront accepter lorsqu'elles requerront une signature électronique.
Finalement, pour éviter un foisonnement d'actes d'exécution, les thèmes pour lesquels un acte pourrait être adopté, seront regroupés dans un nombre minimal d'actes.

Quel sera le rôle de la Commission ?

Hormis pour les actes obligatoires, la Commission décidera de l'opportunité d'adopter tel ou tel acte optionnel en fonction de l'évolution du marché et de problèmes résiduels d'interopérabilité. A cette fin, la Commission consultera les parties prenantes. Formellement, l'adoption des actes secondaires ne sera possible qu'après l'entrée en vigueur du règlement. La Commission en coopération avec les Etats membres a néanmoins commencé les travaux préparatoires à la rédaction des actes obligatoires.

Les organismes de normalisation continueront à travailler en étroite concertation avec la Commission dans le but de disposer de normes répondant aux exigences du règlement. L'Agence Européenne chargée de la sécurité des réseaux et de l'information, jouera aussi un rôle important pour rédiger des lignes directrices à l'attention des prestataires de services pour la mise en œuvre des notifications de brèches de sécurité et pour la gestion des risques. Par ailleurs, elle jouera son rôle de gardienne des Traités en surveillant la bonne exécution du règlement.

Finalement, la Commission produira tous les quatre ans un rapport sur l'examen de l'application du règlement eIDAS et de la réalisation de ses objectifs.

Conférences – Formations :

FNTC, Assises de la Confiance, *Table ronde sur le Thème « Confiance Numérique et règles juridiques : comment profiter des nouvelles réglementations européennes »,* Présentation et animation par Eric A. CAPRIOLI, 16 juin 2014, Paris, www.fntc.org.

FNTC, *Formation sur le droit de la dématérialisation,* Eric A. CAPRIOLI et Pascal AGOSTI, 19 et 20 juin 2014, Paris.
http://www.fntc.org/fr/formations/agenda/event/365-formation-droit-de-la-dematerialisation-des-documents-dr/.

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 .

Note bibliographique

Signature électronique et dématérialisation – Eric A. CAPRIOLI – Droit & Professionnels – LexisNexis –2014

Cet ouvrage didactique fait un tour complet, quasi exhaustif, des règles internes, européennes et internationales applicables en matière de signature électronique, de dématérialisation, d'archivage des documents, qu'il s'agisse de contrats, de bulletin de paie, de factures…

La première partie de l'ouvrage traite de l'identification, de l'authentification et des identités numériques, phase nécessaire pour imputer une action à une personne déterminée. La deuxième renvoie au régime juridique de l'ensemble des services de confiance dans les transactions électroniques comme la signature électronique, le cachet, les contremarques de temps, les services de fourniture électronique (lettre recommandée électronique)…La dernière est consacrée au régime juridique des prestataires de services de confiance (obligations et responsabilités) ainsi que les conditions de certification/de qualification des services et prestataires…

Cet ouvrage riche en références et jurisprudences permet d'approfondir certains points … A mettre d'urgence entre toutes les mains.

La minute nécessaire…

Du numérique au digital

A la fin de l'année dernière, l'Académie française a rappelé que « *L'adjectif digital en français signifie « qui appartient aux doigts, se rapporte aux doigts ». Il vient du latin digitalis, « qui a l'épaisseur d'un doigt », lui-même dérivé de digitus, « doigt ». C'est parce que l'on comptait sur ses doigts que de ce nom latin a aussi été tiré, en anglais, digit, « chiffre », et digital, « qui utilise des nombres ». On se gardera bien de confondre ces deux adjectifs digital, qui appartiennent à des langues différentes et dont les sens ne se recouvrent pas : on se souviendra que le français a à sa disposition l'adjectif numérique. ».*

Pourtant, la pratique ne peut s'empêcher de mêler les deux dès lors que le monde du numérique adore emprunter à l'anglais, rendant notre langage truffé d'anglicismes. Mais au-delà de cette modification syntaxique, c'est un glissement sémantique qui fait jour. Désormais de nombreuses directions sont débaptisées : l'entreprise numérique devient digitale et la dématérialisation devient la digitalisation…On se rend compte qu'en fait, selon les termes employés, ce sont deux mondes qui s'affrontent : le Numérique renverrait à l'adaptation de concepts ou comportements existants dans le monde « réel » (comme la signature, l'écrit…) tandis que le Digital aurait trait à des actions originellement virtuelles (donc sans transposition du réel vers le virtuel) comme les like, post, murs, wiki, Open…

En ce sens, le Droit doit s'adapter (ce qui ne signifie pas une inflation législative dans le domaine) pour prendre en compte cette dichotomie sans cesse plus flagrante. Par de la Soft Law (Ex : Chartes, Netiquette, CGU…) bien sûr. Mais aussi par une façon différente de penser le Droit, plus collaborative.

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