

LA LETTRE DU CABINET

TECHNOLOGIES DE L'INFORMATION

EDITO

Nous avons le plaisir de vous adresser le dix-huitième numéro de notre Newsletter.

Cette lettre est organisée autour des thématiques suivantes : deux flash spéciaux pour l'adoption de la loi pour une République numérique et pour l'entrée en vigueur de la réforme du droit des contrats, puis des points sur la réglementation ou la jurisprudence dans les domaines du droit de l'informatique, de l'internet, de la protection des données personnelles, de la propriété intellectuelle, les médias numériques, la santé numérique, la robotique, la cybersécurité, le droit des affaires et le droit fiscal, et enfin la vie du Cabinet. Nous souhaitons par ce moyen vous informer des derniers développements du droit des technologies de l'information.

Si vous le souhaitez, merci de nous faire part de vos impressions, critiques ou suggestions.

Nous vous souhaitons une bonne lecture.

SOMMAIRE

① FLASH (P. 2-3)

- PROMULGATION DE LA LOI POUR UNE RÉPUBLIQUE NUMÉRIQUE

- ENTRÉE EN VIGUEUR DE LA RÉFORME DU DROIT DES CONTRATS

INFORMATIQUE (p.3-6)

Réglementation

- Publication du rapport sur l'ouverture des données publiques dans les collectivités locales

Jurisprudence

- La revente de la copie de sauvegarde d'un logiciel est interdite, sauf accord du titulaire

- La vente d'un ordinateur équipé de logiciels préinstallés n'est pas déloyale

- La Macif condamnée à plus d'1,5 million d'euros pour rupture abusive d'un contrat d'intégration

- Oracle condamnée en appel pour mauvaise foi et déloyauté en matière d'audit de licence de logiciels

- Le non-paiement de factures par le client ne peut justifier la rétention du code d'accès au serveur par le prestataire

INTERNET (p.6-7)

Réglementation

- Le gouvernement américain met un terme à la gouvernance de l'Icann

Jurisprudence

- Amazon ne peut imposer la loi applicable dans ses CGV aux consommateurs

PROTECTION DES DONNÉES PERSONNELLES (p.7-9)

Réglementation

- L'accord « EU-US Privacy Shield » sur le transfert de données vers les Etats-Unis est confirmé par la Commission européenne

Jurisprudence

- Le droit d'opposition d'une personne sur ses données (nom, prénom) ne peut restreindre la liberté de la presse

PROPRIÉTÉ INTELLECTUELLE ET MARQUES (p.9)Réglementation

- Projet de réforme européenne du droit d'auteur

MÉDIAS NUMÉRIQUES (p.9-10)Réglementation

- Proposition de révision de la directive sur les services de médias audiovisuels

SANTÉ NUMÉRIQUE (p.10)Réglementation

- Publication de deux décrets d'application de la loi de modernisation de notre système de santé

ROBOTIQUE (p.10)Réglementation

- Nouvelle loi relative au renforcement de la sécurité de l'usage des drones civils

CYBERSÉCURITÉ (p.11)Réglementation

- Publication de la directive sur la sécurité des réseaux et des systèmes d'information

DROIT DES AFFAIRES (p.11)Jurisprudence

- La rupture, même prévisible, d'une relation commerciale établie est brutale en l'absence de préavis écrit

DROIT FISCAL ET E-COMMERCE (p.12)Réglementation

- Nouvelles obligations déclaratives à la charge des plateformes de mise en relation

VIE DU CABINET (p.12)**📢 FLASH – PROMULGATION DE LA LOI POUR UNE RÉPUBLIQUE NUMÉRIQUE**

La loi pour une République numérique a finalement été adoptée le 7 octobre 2016. En résumé, les dispositions de la loi sont organisées selon trois grands axes :

1) *L'open data* : la loi prévoit l'ouverture par défaut d'une partie des données publiques des administrations, des données d'organismes ayant une mission de service public ainsi que le libre accès aux données de recherche publique et l'accès sécurisé des chercheurs aux grandes bases de données publiques.

2) *La gouvernance d'internet* : la loi comprend des dispositions relatives à la protection des données personnelles, la loyauté des plateformes et l'encadrement juridique des avis en ligne de consommateurs, la neutralité du net (ou "l'accès non discriminé à internet"). La loi inclut par ailleurs de nouvelles dispositions pénales pour lutter contre les atteintes à l'intimité sexuelle (notamment, la pratique du "revenge porn"). Concernant la protection des données personnelles, la loi modifie et complète la loi Informatique et Libertés en créant de nouveaux droits (droit à l'oubli pour les mineurs), en anticipant l'entrée en vigueur du Règlement général pour la protection des données (RGPD) en intégrant certaines de ses dispositions (portabilité et récupération des données, augmentation du montant des sanctions administratives pouvant être appliquées par la CNIL à trois millions d'euros) et en élargissant les compétences de la CNIL.

3) *L'accessibilité numérique* : ce troisième axe concerne l'accélération de la couverture en très haut débit sur le territoire et les obligations d'accessibilité numérique, permettant à tous les utilisateurs de pouvoir accéder aux contenus numériques. Cette partie prévoit également la reconnaissance de l'"e-sport" et crée un statut social pour les joueurs professionnels. (*Loi n°2016-1321 du 7 octobre 2016 pour une République numérique*)

📢 FLASH – ENTRÉE EN VIGUEUR DE LA RÉFORME DU DROIT DES CONTRATS

Le 1er octobre 2016 est entrée en vigueur la réforme du droit des contrats, issue de l'ordonnance du 10 février 2016. Cette réforme majeure a pour effet d'intégrer dans le code civil de nombreux concepts développés par la jurisprudence au fil des ans. Le droit des contrats en ressort modernisé. La consécration de la jurisprudence le rend plus lisible. Enfin, cette réforme emporte une refonte du code

civil avec une large renumérotation et une réorganisation des articles relatifs au contrat.

Les principales évolutions peuvent être résumées comme suit :

- *La période pré-contractuelle et la formation du contrat*

De nouvelles dispositions sont consacrées aux négociations (art. 1112 et s. c.civ.) : principe de liberté des négociations, exigence de bonne foi pesant sur les négociateurs, devoir général d'information et obligation de confidentialité.

La formation du contrat et les notions d'offre et d'acceptation sont désormais codifiées (art. 1113 à 1122).

- *La période contractuelle*

Les notions relatives aux vices du consentement ont été modifiées et certaines précisions jurisprudentielles codifiées (art. 1130 et s.).

Concernant le contenu du contrat, qui doit être conforme à l'ordre public, la notion de clause abusive est prévue à l'article 1171.

Concernant les effets du contrat, l'ordonnance consacre la théorie de la révision pour imprévision (art. 1195). Des règles générales sur la durée du contrat sont introduites dans le code (art. 1210 s.), ainsi que des règles sur la cession du contrat (art 1216 s.), sur l'inexécution contractuelle (art. 1217 s.) et sur la résolution (art. 1224 et s.).

Ce nouveau droit des contrats ne s'appliquera qu'aux contrats conclus à compter du 1er octobre 2016.

Les contrats informatiques seront notamment impactés par ces nouvelles dispositions. Les contrats conclus avant cette date resteront soumis aux règles applicables avant le 1er octobre. (Ordonnance n°2016-131 du 10 février 2016 portant réforme du droit des contrats, du régime général et de la preuve des obligations)

INFORMATIQUE

RÉGLEMENTATION

Open Data - Publication du rapport sur l'ouverture des données publiques dans les collectivités locales

La réutilisation des données publiques doit permettre aux organismes publics et privés de développer de nouveaux outils de communication et des services à destination des citoyens. Une politique Open data est en oeuvre depuis plusieurs années en France. Par ailleurs, la loi du 7 octobre 2016 pour une République numérique prévoit la généralisation de la publication en ligne des principales données publiques de l'Etat et des collectivités locales de plus de 3500 habitants d'ici 2018.

Le rapport, rédigé à la demande des secrétaires d'Etat Axelle Lemaire et Estelle Grelier, par Opendata France, avec le concours de la mission Etalab, a été remis le 17 octobre dernier.

Ce document dresse un état des lieux de l'ouverture des données publiques dans les territoires. Ainsi, plus de 10.000 jeux de données ont déjà été mis en ligne par une centaine de collectivités locales, notamment grâce à la plateforme nationale data.gouv.fr. Des disparités importantes subsistent cependant entre les grandes collectivités et les communes de plus petite taille, qui manquent de ressources pour mettre en oeuvre une réelle politique d'open data. Enfin, il est nécessaire de renforcer la normalisation des données, leur interopérabilité et leur réutilisation par les acteurs publics et privés pour créer de nouveaux services.

Le rapport d'Opendata France formule plusieurs recommandations :

- Soutenir l'effort des collectivités par une "dotation de données" de la part de l'Etat avec la création d'une API ouverte à l'ensemble des collectivités, pour leur permettre de générer automatiquement la version locale des données nationales déjà publiées en open data ;
- Définir avec les collectivités locales un "socle commun de données", qui devront être ouvertes en priorité, tel que les budgets, les résultats électoraux, les plans locaux d'urbanisme (PLU), ou les données de transports ;
- Créer des outils pour la formation à l'open data et certifier les formateurs ;
- Mettre en place ces dispositifs par le biais d'une expérimentation dans une dizaine de territoires pilotes. (*Rapport sur les dispositifs d'accompagnement des collectivités locales à l'ouverture des données publiques, 17 octobre 2016, disponible sur le site du Minefi*)

JURISPRUDENCE

Logiciel – La revente de la copie de sauvegarde d'un logiciel est interdite, sauf avec l'accord du titulaire

Dans son arrêt UsedSoft rendu en 2012, la Cour de Justice de l'Union européenne (CJUE), avait confirmé les dispositions de la directive de 1991 sur la protection juridique des programmes

d'ordinateur selon lesquelles, l'acquéreur initial d'un exemplaire d'un programme d'ordinateur peut le revendre d'occasion à un sous-acquéreur, en application de la règle de l'épuisement du droit de distribution, et sous certaines conditions.

En effet, en application de la règle de l'épuisement du droit de distribution, le titulaire des droits d'auteur sur un programme d'ordinateur, qui distribue ce programme sur un support physique (CD-ROM par exemple) dans l'Union européenne en vertu d'une licence d'utilisation illimitée, ne peut plus s'opposer aux reventes ultérieures de ces copies par l'acquéreur initial ou les acquéreurs successifs, quand bien même le contrat de licence interdirait toute cession ultérieure du programme.

Cependant, l'arrêt UsedSoft ne portait que sur l'exemplaire du logiciel fourni à l'acquéreur initial, et non la copie de sauvegarde. Dans un arrêt du 12 octobre 2016, la CJUE vient de se prononcer sur ce point.

L'espèce concernait deux revendeurs situés en Lettonie, qui entre 2001 et 2004 ont revendu en ligne plus de 3.000 copies de sauvegarde de plusieurs logiciels Microsoft. Les deux revendeurs ont été poursuivis au pénal pour vente illégale en bande organisée d'objets couverts par le droit d'auteur et utilisation illégale de la marque d'autrui. La cour de Riga, en charge de l'affaire a posé deux questions préjudicielles à la CJUE afin de déterminer si la règle de l'épuisement du droit de distribution et donc le droit de revendre des programmes d'ordinateur, était étendu aux copies de sauvegarde, notamment lorsque le programme d'origine a été effacé ou endommagé.

À cet égard, la Cour rappelle que la directive prévoit qu'une personne ayant le droit d'utiliser un programme d'ordinateur ne peut être empêchée par contrat d'en faire une copie de sauvegarde dans la mesure où une telle copie est nécessaire pour cette utilisation. Selon la Cour, cette règle, qui établit une exception au droit exclusif de reproduction du titulaire du droit d'auteur d'un programme d'ordinateur, doit cependant faire l'objet d'une interprétation stricte. En conséquence, l'utilisateur ne peut réaliser et utiliser une copie de sauvegarde que pour répondre à ses seuls besoins.

La Cour conclut que "si l'acquéreur initial de la copie d'un programme d'ordinateur accompagnée d'une licence d'utilisation illimitée est en droit de revendre d'occasion cette copie et sa licence à un sous-acquéreur, il ne peut en revanche, lorsque le support physique d'origine de la copie qui lui a été initialement délivré est endommagé, détruit ou égaré, fournir à ce sous-acquéreur sa copie de sauvegarde de ce programme sans l'autorisation du titulaire du droit." (CJUE, 3ème ch., 12 oct. 2016, aff. C-166/15, *Ranks et Vasiļevičs c. Microsoft Corp.* ; et voir CJUE, Gde ch., 3 juil. 2012, aff. C-128-11, *Arrêt UsedSoft GmbH c. Oracle International Corp.*)

Vente liée – La vente d'un ordinateur équipé de logiciels préinstallés non déloyale selon la CJUE

Dans un arrêt du 7 septembre 2016, la Cour de justice de l'Union européenne a jugé que la vente d'un ordinateur équipé de logiciels préinstallés ne constituait pas, en soi, une pratique commerciale déloyale. De plus, l'absence d'indication du prix de chacun des logiciels préinstallés ne constitue pas une pratique commerciale trompeuse. Cet arrêt nuance la décision de la Cour de cassation du 5 février 2014 selon laquelle la vente d'un ordinateur équipé de logiciels préinstallés ne constituait pas une pratique commerciale déloyale, dès lors que le consommateur pouvait se procurer un ordinateur "nu" auprès du fabricant.

En l'espèce, un consommateur français avait acheté un ordinateur équipé de logiciels préinstallés. L'acheteur a alors demandé au fabricant de lui rembourser le prix d'achat des logiciels. Le fabricant a proposé d'annuler la vente et de lui rembourser le prix d'achat. L'acheteur a refusé et a ensuite décidé d'assigner le fabricant devant les tribunaux français sur le fondement des dispositions du code de la consommation relatives aux pratiques commerciales déloyales et notamment les pratiques altérant le comportement économique des consommateurs et contraires aux exigences de la diligence professionnelle. La Cour de cassation, saisie de l'affaire, a posé plusieurs questions préjudicielles à la CJUE, à savoir si l'absence d'indication du prix de chacun des logiciels préinstallés, l'impossibilité pour le consommateur d'acheter un ordinateur non équipé chez le même fabricant, et l'absence de choix pour le consommateur d'accepter les logiciels préinstallés ou d'obtenir la révocation de la vente doivent être considérées comme des pratiques déloyales au sens de la directive 2005/29/CE sur les pratiques commerciales déloyales.

La CJUE considère que la vente d'un ordinateur équipé de logiciels préinstallés, sans possibilité pour le consommateur de se procurer le même modèle sans ces logiciels n'est pas, en soi, une pratique déloyale, sous réserve que l'offre ne soit pas contraire aux exigences de la diligence professionnelle et qu'elle n'altère pas de manière substantielle le comportement du consommateur moyen par rapport au produit. Il reviendra aux tribunaux d'apprécier au cas par cas les circonstances de la vente, à savoir : l'information correcte du consommateur, la conformité de l'offre conjointe aux attentes d'une part notable des consommateurs, et la possibilité pour le consommateur d'accepter l'offre ou d'obtenir la révocation de la vente.

Considérant l'absence d'indication des prix des logiciels préinstallés, la Cour estime que cette pratique commerciale n'est pas trompeuse. En effet, pour la Cour, le prix global d'un produit est une information substantielle que le professionnel est obligé d'indiquer, et non le prix de chacun des éléments. Le prix de chaque logiciel préinstallé ne constitue pas une information substantielle. (CJUE, 7 sept. 2016, aff. C-310/15, *Deroo-Blanquart c. Sony Europe Ltd*)

Contrat - Rupture abusive d'un contrat d'intégration par la Macif

Par jugement du 24 juin 2016, le tribunal de commerce de Nanterre a condamné la Macif pour la résiliation abusive d'un contrat d'intégration d'une solution logicielle éditée par la société IGA Assurances et du contrat de licence-maintenance.

Dans le cadre de la réorganisation de sa filiale Macifilia, la Macif avait souhaité remplacer l'application informatique de gestion d'activités d'assurance. Elle a donc lancé un appel d'offres, remporté par la société IGA Assurances. Après la conclusion d'un contrat de cadrage pour l'analyse des besoins afin de préciser le périmètre fonctionnel du projet, les parties ont signé un contrat d'intégration pour la livraison d'une solution logicielle ainsi qu'un contrat de concession de droit d'utilisation du progiciel et de maintenance. Suite à de nombreux retards, la Macif a mis IGA Assurances en demeure de livrer l'ensemble des spécifications fonctionnelles détaillées (SFD) sous 30 jours. IGA Assurances s'est exécutée, en précisant que 62 SFD sur les 75 de la V1 avaient été livrées. Considérant qu'IGA Assurances n'avait pas respecté le délai imparti et que la livraison ne couvrait pas la totalité des besoins exprimés, la Macif a résilié le contrat pour faute grave et répétée d'IGA Assurances.

Le tribunal constate qu'aucune stipulation contractuelle n'impose à IGA Assurances de couvrir l'intégralité des besoins de la matrice par des spécifications fonctionnelles détaillées. Son obligation de résultat se limite aux spécifications indispensables aux développements et aux adaptations à apporter à la version de base de la solution. Pour caractériser un défaut de livraison sur le plan quantitatif, la Macif aurait dû indiquer précisément quelles spécifications n'avaient pas couvert un besoin destiné à un développement spécifique. Par ailleurs, le tribunal a jugé que la Macif avait insuffisamment justifié le défaut de qualité des SFD, et qu'il n'était pas uniquement imputable à IGA Assurances. De même, le tribunal considère que la Macif n'a pas justifié le non-respect des délais de réalisation, qualifiés d'obligation essentielle du contrat d'intégration. Enfin, le tribunal a jugé que la Macif avait manqué à son obligation de coopération de bonne foi dans l'exécution du contrat d'intégration. En conséquence, le contrat d'intégration est résolu aux torts exclusifs de la Macif, ainsi que le contrat de licence-maintenance.

Pour la demande de réparation d'IGA Assurances, le tribunal a appliqué les règles de calcul fixées par le contrat d'intégration. Ces montants s'élèvent à 1.147.846€, auxquels s'ajoutent le règlement d'une facture impayée de 276.000€ et 226.190€ au titre de l'article 700 du code de procédure civile, soit un total de 1.650.000€. (*T. com. Nanterre, 4^{ème} ch., jugement du 24 juin 2016, Macif c. IGA Assurances*)

Audit de licences de logiciels - Oracle condamné en appel pour mauvaise foi et déloyauté

La cour d'appel de Paris, statuant sur l'appel du jugement du Tribunal de grande instance de Paris du 6 novembre 2014, a confirmé la condamnation de la société Oracle pour ses pratiques agressives en matière d'audit de licences de logiciels.

L'Association nationale pour la formation professionnelle des adultes (AFPA) a attribué en 2002 un marché de fourniture de services informatiques à l'intégrateur Sopra Group (devenu Sopra Steria), prestataire agréé de la société Oracle. Cette société avait remporté l'appel d'offres avec la solution Oracle E-Business Suite. Le marché a pris fin en 2005. Lors de la reprise des contrats par la société Oracle, celle-ci a décidé d'organiser deux audits de licences. Le second audit a été suspendu alors que l'AFPA lançait un nouvel appel d'offres auquel la société Oracle a décidé de répondre. Le nouveau contrat ne lui ayant pas été attribué, la société Oracle a repris l'audit qu'elle avait suspendu. A l'issue de cet audit, Oracle a conclu que l'AFPA utilisait 885 licences du logiciel Purchasing sans en avoir acquis les droits car selon Oracle, ce logiciel faisait partie d'une autre suite logicielle.

Après deux ans de négociations infructueuses, les sociétés Oracle Corporation, Oracle International Corporation et Oracle France ont assigné l'AFPA pour contrefaçon du logiciel Purchasing pour lequel l'AFPA n'aurait pas acquis les droits d'exploitation. L'AFPA a alors appelé en garantie la société Sopra Group.

Pour sa défense, l'AFPA explique que le logiciel Purchasing était intégré dans la suite logicielle Financials, objet du premier marché de fourniture accordé à Sopra Group. L'AFPA indiquait par ailleurs que si le tribunal devait en juger autrement, le contrat a toutefois été exécuté de bonne foi car le logiciel Purchasing avait été installé sur son système informatique par Sopra, prestataire agréé d'Oracle.

D'après les juges du fond, la question posée ne relevait pas du droit d'auteur, mais du droit des

contrats. En effet, le tribunal a jugé qu'il "n'est à aucun moment soutenu que l'AFPA aurait utilisé un logiciel cracké ou implanté seule un logiciel non fourni par la société Sopra Group, ni même que le nombre de licences ne correspondait pas au nombre d'utilisateurs. En conséquence, le litige soumis au tribunal n'est pas un litige de contrefaçon mais bien un litige portant sur le périmètre du contrat et sur sa bonne ou sa mauvaise exécution."

La cour d'appel va cependant infirmer le jugement sur le fondement de la demande. Contrairement au TGI, la cour considère la demande en contrefaçon recevable et examine si l'AFPA et Sopra avaient manqué à leurs obligations contractuelles en installant et en utilisant le logiciel Purchasing. La cour a estimé "qu'en installant et en utilisant le module PO, se rattachant pour le moins au logiciel Purchasing et inclus dans le périmètre du marché Mosaïc, lequel a été dûment payé, la société Sopra Group et l'AFPA n'ont manqué à aucune de leurs obligations contractuelles ; qu'aucun acte de contrefaçon ne peut donc leur être reproché par la société Oracle International Corporation".

La cour a en revanche retenu les demandes reconventionnelles en dommages-intérêts de l'AFPA et de Sopra pour avoir agi avec mauvaise foi et déloyauté envers ces deux organisations. Elle a estimé qu'Oracle avait profité à deux reprises de son droit contractuel de procéder à des audits, de manière à faire pression et obtenir la souscription de nouvelles licences incluses dans l'offre de 2001.

Les sociétés Oracle Corporation, Oracle International Corporation et Oracle France sont condamnées à verser 100.000 € à l'AFPA et la même somme à Sopra au titre des dommages-intérêts et 100.000 € à chacune au titre de l'article 700 (frais de procédure). L'arrêt fait l'objet d'un pourvoi en cassation. (CA Paris, pôle 5, ch. 1, arrêt du 10 Mai 2016, Oracle France, Oracle Corporation, Oracle International Corporation / AFPA, Sopra Steria Group)

Contrat - Le non-paiement de factures par le client ne peut justifier la rétention du mot de passe d'accès au serveur par le prestataire

Par une ordonnance de référé du 4 octobre 2016, le tribunal de grande instance de Laval a ordonné à un prestataire informatique de remettre à son ancien client le mot de passe permettant l'accès au serveur de son infrastructure. Le prestataire avait en effet conditionné la remise de ce mot de passe au paiement des factures dues.

En l'espèce, la société Belliard avait fait appel à la société Kirsch, prestataire informatiques, pour gérer ses installations informatiques en réseau et développer un logiciel de gestion. Mécontente du développement, la société Belliard a refusé de payer plusieurs factures puis a fait appel à un nouveau prestataire. Celui-ci a constaté que l'ancien prestataire avait modifié le mot de passe permettant l'accès au serveur de l'infrastructure. La société Belliard a donc mis en demeure la société Kirsch de communiquer le mot de passe. Cette dernière lui a répondu qu'elle le communiquerait contre paiement des factures et la remise d'une décharge de responsabilité concernant l'état du logiciel en cours de développement. La société Belliard a assigné la société Kirsch en référé pour obtenir le mot de passe.

Le juge des référés a considéré que "le non-paiement des factures litigieuses ne pouvait justifier le refus de la société Kirsch de communiquer le code d'accès à l'installation". Il a cependant ordonné au client de payer les factures de maintenance, non contestées. Concernant les factures relatives au développement du logiciel, il reviendra à la juridiction du fond de statuer sur l'exécution du contrat. (TGI de Laval, ordonnance de référé du 4 octobre 2016, Belliard c. Kirsch)

INTERNET

RÉGLEMENTATION

ICANN - Fin de la gouvernance d'internet par l'administration américaine

Malgré les tentatives de blocage de plusieurs parlementaires américains, dont le sénateur du Texas Ted Cruz, le contrat de la NTIA (Administration nationale des télécommunications et de l'information - dépendant du Department of Commerce américain) pour la supervision de l'Icann (Internet Corporation for Assigned Names and Numbers) a pris fin le 30 septembre 2016. L'Icann est désormais supervisé par la Communauté Globale de l'Internet (Global Internet Community). Le nouveau modèle de gouvernance de l'Icann repose sur l'intégration de parties prenantes de tous horizons : entreprises, universitaires, experts techniques, membres de la société civile, représentants de gouvernements, etc.

Selon Ed Black, président et CEO de la Computer and Communications Industry, le processus de transition pour "assurer la stabilité à long terme de l'internet et pérenniser un internet ouvert, dont le fonctionnement a des répercussions directes sur l'économie et la sécurité nationale" des États-Unis, devait aller à son terme. Cependant, pour ses opposants, la fin de la supervision de la NTIA crée le

risque de voir l'Icann victime "de toute influence indue ou de toute appropriation par des gouvernements, des organisations multilatérales ou intergouvernementales, ou des parties prenantes commerciales ou non commerciales", mettant en péril les libertés sur internet.

L'Icann assure que les utilisateurs ne verront aucun changement dans leur utilisation d'internet après cette transition. (Voir notamment "Icann : la transition aura lieu malgré le blocage de certains sénateurs US" in *Le Monde Informatique*, 14 septembre 2016 et site de l'ICANN à www.icann.org)

JURISPRUDENCE

CGV et loi applicable - Amazon ne peut imposer la loi applicable dans ses CGV aux consommateurs

Dans un arrêt du 28 juillet 2016, opposant une association autrichienne de protection des consommateurs à Amazon EU Sarl, la Cour de justice de l'Union européenne (CJUE) s'est prononcée sur la loi applicable, d'une part, aux conditions générales de vente et d'utilisation d'Amazon (version de 2012) qui désignaient la loi luxembourgeoise et d'autre part, à son traitement automatisé de données.

Le litige portait sur plusieurs clauses des CGU/CGV conclues entre Amazon EU et les consommateurs/utilisateurs de ses services, notamment la clause relative à la loi applicable. La société Amazon EU a son siège à Luxembourg et exploite plusieurs sites web, dont un site avec l'extension .de visant notamment le marché autrichien. La Cour suprême autrichienne, saisie du litige, a posé plusieurs questions préjudicielles à la CJUE concernant la loi applicable aux contrats, au caractère abusif de cette clause, et sur la loi applicable au traitement automatisé de données d'Amazon EU.

Pour déterminer si Amazon peut imposer dans ses CGU/CGV la loi luxembourgeoise aux consommateurs européens, la Cour a examiné les règlements Rome I pour les obligations contractuelles (CGV et CGU) et Rome II pour les obligations non contractuelles (action en cessation, permettant de faire cesser ou interdire une infraction nuisant aux intérêts collectifs des consommateurs).

S'agissant des obligations contractuelles et de la loi applicable à l'appréciation d'une clause contractuelle abusive, la Cour considère que la loi applicable doit toujours être déterminée en application du règlement européen "Rome I". Selon ce règlement, la loi applicable est celle du pays de résidence du consommateur. La Cour a toutefois rappelé les critères d'appréciation du caractère abusif. Selon le règlement "Rome I", les parties peuvent choisir le droit applicable à un contrat de consommation, "à condition que soit assuré le respect de la protection dont le consommateur bénéficie en vertu des dispositions de la loi de son for auxquelles il ne peut être dérogé par accord". Il en résulte qu'une clause "figurant dans les conditions générales de vente d'un professionnel, qui n'a pas fait l'objet d'une négociation individuelle, selon laquelle la loi de l'État membre du siège de ce professionnel régit le contrat conclu par voie de commerce électronique avec un consommateur est abusive pour autant qu'elle induise ce consommateur en erreur en lui donnant l'impression que seule la loi de cet État membre s'applique au contrat (...)."

S'agissant ensuite du droit applicable au traitement des données personnelles effectué par Amazon EU, la Cour considère que la loi de l'État membre vers lequel elle dirige ses activités est applicable, s'il s'avère qu'elle procède au traitement des données en question dans le cadre des activités d'un établissement situé dans cet État membre, ce qu'il appartient à la juridiction de renvoi de vérifier.

En conclusion, cet arrêt confirme qu'un site de commerce électronique qui vise plusieurs pays peut être poursuivi par un consommateur devant la juridiction de son pays de résidence, malgré la désignation de la loi applicable dans les CGV. Par ailleurs, le traitement de données personnelles sera susceptible d'être soumis au droit de plusieurs pays, suivant les États membres vers lesquels les activités commerciales sont dirigées. Sur ce dernier point, l'entrée en application du règlement général sur la protection de données (mai 2018) aura un effet unificateur. (CJUE, 3^e ch., 28 juill. 2016, aff. C-191/15, *Verein für Konsumenteninformation c. Amazon EU sarl*)

PROTECTION DES DONNÉES PERSONNELLES

RÈGLEMENTATION

Transfert de données vers les Etats-Unis – L'accord Privacy Shield adopté par la Commission européenne

En discussion depuis la décision d'invalidité du Safe Harbor en octobre 2015, le Privacy Shield - ou Bouclier de protection des données, visant à encadrer les conditions de transfert des données personnelles de citoyens de l'Union européenne vers les Etats-Unis, a été adopté par la Commission

européenne le 12 juillet 2016.

Pour rappel, le Privacy Shield remplace le système de Safe Harbor, permettant de transférer des données personnelles de citoyens européens vers des sociétés américaines adhérant au programme. Le Safe Harbor avait été invalidé par la Cour de justice de l'Union européenne avec l'arrêt Schrems du 6 octobre 2015.

Selon la Commission européenne, ce nouveau cadre *“protège les droits fondamentaux de tout citoyen de l'UE dont les données à caractère personnel sont transférées vers les Etats-Unis tout en apportant de la clarté juridique aux entreprises qui ont recours à des transferts de données transatlantiques.”* La Commission souligne également que dans le cadre de cet accord, les Etats-Unis s'engagent à exclure toute surveillance de masse systématique des données à caractère personnel transférées vers leur territoire.

Comme le Safe Harbor, le Privacy Shield fonctionne sur un système de volontariat et ne s'applique qu'aux sociétés américaines ayant décidé d'y adhérer et de se conformer à ses prescriptions. Depuis le 1er août, les sociétés américaines adhérentes peuvent s'enregistrer auprès de Département du commerce américain pour bénéficier des conditions du Privacy Shield. Le Département du commerce s'est engagé à contrôler régulièrement que les entreprises adhérentes respectent effectivement leurs obligations. Notamment, en cas de re-transfert des données vers un pays tiers, les entreprises adhérentes doivent s'assurer que les parties tierces "assurent le même niveau de protection".

La Commission va publier un guide à destination des citoyens européens décrivant comment adresser une plainte aux autorités en cas d'utilisation non conforme de leurs données.

Les engagements figurant dans le nouveau Privacy Shield ne rassurent pas tous les utilisateurs européens dont les données personnelles sont transférées aux Etats-Unis. Certaines organisations, telles les associations de défense des droits civils sur internet, ou certaines organisations de consommateurs s'élèvent déjà contre un accord qu'elles jugent insuffisant.

Le Privacy Shield n'est pas un texte figé. Cet accord devrait en effet faire l'objet de révisions annuelles. Ces révisions porteront notamment sur la collecte automatique de données et le "profilage", pratiques non couvertes par l'accord. Ces révisions font également l'objet de critiques, donnant lieu à des craintes sur des modifications à venir, remettant en cause les principes de cet accord. Face au risque d'incertitude sur la pérennité et la stabilité du Privacy Shield ainsi que les craintes d'utilisateurs, certaines entreprises ont choisi de soumettre leurs politiques de transfert de données personnelles vers les Etats-Unis aux autres outils disponibles (clauses contractuelles types par exemple), voire de transférer ou de créer des centres d'hébergement de données au sein de l'Union européenne (voir l'exemple de la société Salesforce).

L'accalmie autour du débat sur les transferts de données vers les Etats-Unis n'est toutefois que temporaire. Ainsi, les tribunaux irlandais ont envoyé un nouveau dossier devant la CJUE aux fins d'examiner la validité des clauses contractuelles types. Ces clauses contractuelles, publiées par la Commission, permettent aux entités les ayant signées, de transférer des données vers les Etats-Unis ou d'autres pays tiers. Or, depuis l'annulation du Safe Harbor, certains remettent également en cause les clauses contractuelles types. (*“La Commission européenne lance le bouclier de protection des données UE-États-Unis: une protection renforcée pour les flux de données transatlantiques”, communiqué de presse de la Commission européenne du 12 juillet 2016*)

JURISPRUDENCE

Données personnelles - Le droit d'opposition ne peut restreindre la liberté de la presse

Dans un arrêt du 12 mai 2016, la Cour de cassation a affirmé que la demande de retrait des noms et prénoms d'un particulier du site d'une publication de presse, au nom du droit à s'opposer à ce que les données personnelles fassent l'objet d'un traitement, excède les restrictions qui peuvent être rapportées à la liberté de presse.

Dans cette affaire, deux frères avaient assigné le quotidien Les Echos pour que soit ordonnée la suppression de leur nom de famille dans le moteur de recherche du site LesEchos.fr, permettant d'accéder à un article publié en 2006, archivé sur son site avec le titre "Le Conseil d'Etat a réduit la sanction des frères X à un blâme". Ces derniers fondaient leur demande sur l'article 38 de la loi Informatique et Libertés relatif au droit d'opposition au traitement de données à caractère personnel.

La Cour a estimé que *“le fait d'imposer à un organe de presse, soit de supprimer du site internet dédié à l'archivage de ses articles, (...) l'information elle-même contenue dans l'un de ces articles, le retrait des nom et prénom des personnes visées par la décision privant celui-ci de tout intérêt, soit d'en restreindre l'accès en modifiant le référencement habituel, excède les restrictions qui peuvent être apportées à la liberté de la presse, la cour d'appel a légalement justifié sa décision”.*

Dans une ordonnance de référé du 8 janvier 2016, le TGI de Paris s'était prononcé sur une demande de suppression des nom et prénom d'une personne citée dans un article en ligne du journal 20minutes

et avait également fait primer la liberté d'expression. (C cass., ch. civ. 1, arrêt du 12 mai 2016, MM. Stéphane et Pascal X c. Les Echos)

PROPRIÉTÉ INTELLECTUELLE

RÉGLEMENTATION

Projet de réforme européenne du droit d'auteur

Le 14 septembre 2016, la Commission européenne a proposé deux directives et deux règlements visant à adapter les règles du droit d'auteur aux réalités du marché unique numérique. Ce projet de "paquet droit d'auteur" a été publié conjointement avec une note explicative et une analyse d'impact de la modernisation des règles du droit d'auteur européen.

La proposition de Directive sur le droit d'auteur dans le marché unique numérique et la proposition de Règlement établissant les règles relatives à l'exercice du droit d'auteur et des droits voisins applicables à certaines transmissions en ligne visent à accroître la diversité culturelle et les contenus disponibles en ligne, tout en clarifiant les règles pour tous les acteurs des services en ligne.

Les propositions de la Commission poursuivent trois objectifs prioritaires :

a) permettre un meilleur accès aux contenus en ligne protégés au sein de l'Union européenne, en mettant l'accent sur les programmes de radio et de télévision, les œuvres audiovisuelles européennes et le patrimoine culturel ;

b) faciliter l'utilisation numérique des contenus protégés à des fins telles que l'éducation, la recherche et la conservation dans le marché unique, et

c) améliorer le fonctionnement du marché des droits d'auteur en ligne pour tous les acteurs et contribuer à l'investissement dans des contenus créatifs et à l'innovation dans les modes de diffusion. (Proposition de Directive sur le droit d'auteur dans le marché unique numérique (COM (2016) 593 final) ; Proposition de Règlement établissant les règles relatives à l'exercice du droit d'auteur et des droits voisins applicables à certaines transmissions en ligne des organismes de radiodiffusion et à la retransmission des programmes de télévision et de radio (COM (2016) 594 final)

MÉDIAS NUMÉRIQUES

RÉGLEMENTATION

Proposition de révision de la directive sur les services de médias audiovisuels

Le 25 mai 2016, la Commission européenne a publié une proposition visant à modifier la Directive de 2010 sur les services de médias audiovisuels (Directive SMA). Selon la Commission, l'objectif de cette proposition est de "parvenir à un meilleur équilibre des règles qui s'appliquent aujourd'hui aux organismes traditionnels de radiodiffusion télévisuelle, aux fournisseurs de vidéos à la demande et aux plateformes de partage de vidéos, notamment lorsqu'il s'agit de protéger les enfants. La version révisée de la directive SMA renforce également la promotion de la diversité culturelle européenne, garantit l'indépendance des autorités de régulation de l'audiovisuel et offre une plus grande souplesse aux organismes de diffusion en matière de publicité."

Les principales modifications portent sur les aspects suivants :

Champ d'application : les plateformes de partage de vidéos sont désormais intégrées dans le champ d'application de la Directive. Ces plateformes devront protéger les mineurs contre les contenus préjudiciables et protéger l'ensemble des citoyens contre toute incitation à la haine.

Pays d'origine : ce principe est maintenu, les obligations de transparence sont renforcées et les procédures de détermination du pays compétent sont simplifiées ;

Protection des mineurs : le dispositif existant serait remplacé par des règles communes concernant les contenus qui "pourraient nuire à l'épanouissement physique, mental ou moral des mineurs" et une disposition prévoyant la mise en place de mesures spéciales pour les contenus les plus préjudiciables ;

Œuvres européennes : les obligations des radiodiffuseurs sont maintenues, tandis que celles des services non-linéaires sont renforcées, notamment en ce qui concerne les pays ciblés. Les fournisseurs de contenus à la demande devront veiller à ce que leurs catalogues contiennent au moins 20% de contenus européens. Les Etats membres seront habilités à demander aux services à la demande disponibles dans leur pays de contribuer financièrement à la production d'œuvres européennes ;

Communications commerciales : la proposition prévoit un assouplissement des règles, et le renforcement des codes d'autorégulation et de corégulation ;

Autorités de régulation : le principe de l'indépendance et le renforcement du rôle de l'ERGA sont reconnus, notamment pour l'évaluation de la compétence et l'adoption des codes de l'Union. (Proposition de directive du Parlement européen et du Conseil modifiant la directive 2010/13/UE visant à la coordination de certaines dispositions législatives, réglementaires et administratives des Etats membres relatives à la fourniture de services de médias audiovisuels, compte tenu de l'évolution des réalités du marché (COM(2016)287 final)

SANTÉ NUMÉRIQUE

RÉGLEMENTATION

Données de santé - Publication de deux décrets d'application de la loi de modernisation de notre système de santé

Deux décrets sont parus le 20 juillet 2016, en application de la loi de modernisation de notre système de santé du 26 janvier 2016, notamment aux fins de préciser le champ d'application des articles L.1110-4 et L.1110-12 du Code de la santé publique, relatif à l'échange et au partage des données de santé et à la définition de l'équipe de soins.

Les notions d'échange et de partage de données de santé ont été précisées. Sont ainsi autorisés :

- l'échange entre un ou plusieurs professionnels identifiés, d'informations relatives à une même personne prise en charge, sous réserve de l'information du patient de son droit d'opposition, et à condition que ces professionnels participent tous à sa prise en charge. En outre, ces informations doivent être strictement nécessaires à la coordination ou à la continuité des soins, à la prévention ou au suivi médico-social et social du patient ;

- le partage entre professionnels appartenant à une même équipe de soins, d'informations concernant une même personne qui sont strictement nécessaires à la coordination ou à la continuité des soins ou à un suivi médico-social et social, sous réserve de l'information du patient de son droit d'opposition.

En revanche, le consentement spécifique du patient est requis pour le partage d'informations entre professionnels n'appartenant pas à la même équipe de soins.

Le décret comporte par ailleurs la liste des professionnels entrant dans le champ d'application de l'article L1110-4 du Code de la santé publique autorisés à échanger et partager des données de santé entre eux.

Le second décret du 20 juillet 2016 précise la définition de l'équipe de soins, en application de l'article L1110-12 du Code de la santé publique. Pour rappel l'article L1110-12 définit l'équipe de soins comme "un ensemble de professionnels qui participent directement au profit d'un même patient à la réalisation d'un acte diagnostique, thérapeutique, de compensation du handicap, de soulagement de la douleur ou de prévention de perte d'autonomie, ou aux actions nécessaires à la coordination de plusieurs de ces actes (...)". (Décret n°2016-994 du 20 juillet 2016 relatif aux conditions d'échange et de partage d'informations entre professionnels de santé et autres professionnels des champs social et médico-social et à l'accès aux informations de santé à caractère personnel ; Décret n°2016-996 du 20 juillet 2016 relatif à la liste des structures de coopération, d'exercice partagé ou de coordination sanitaire ou médico-sociale dans lesquelles peuvent exercer les membres d'une équipe de soins)

ROBOTIQUE

RÉGLEMENTATION

Drones - Nouvelle loi relative au renforcement de la sécurité de l'usage des drones civils

La loi du 24 octobre 2016 relative au renforcement de la sécurité de l'usage des drones civils vise à faire évoluer la réglementation de l'usage des drones ("aéronefs opérés ou circulant sans personne à bord"), afin de responsabiliser les usagers et de prévenir les usages indésirables.

Cette nouvelle loi, qui s'applique aux appareils à partir de 800 grammes, prévoit un régime d'enregistrement par voie électronique des drones (au-delà d'un certain poids défini par décret). Les "télépilotes", qui manipulent et contrôlent le pilotage de l'appareil, devront suivre une formation spécifique. Enfin, les drones devront intégrer un dispositif de signalement électronique ou numérique, lumineux et sonore.

Le survol de zones non autorisées par un drone sera sanctionné par une peine maximale d'un an d'emprisonnement et 45.000 euros d'amende, ainsi que la confiscation du drone.

Ces dispositions sont intégrées au Code des transports. (Loi n°2016-1428 du 24 oct. 2016 relative au renforcement de la sécurité de l'usage des drones civils)

CYBERSÉCURITÉ

RÉGLEMENTATION

Cybersécurité - Publication de la directive sur la sécurité des réseaux et des systèmes d'information

Faisant suite à la communication de la Commission européenne du 7 février 2013 intitulée "Stratégie de cybersécurité de l'Union européenne : un cyberspace ouvert, sûr et sécurisé", présentée le 7 février 2013, la directive du 6 juillet 2016 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union européenne vient d'être publiée.

Les principaux points à retenir sont les suivants :

- *L'adoption par les Etats membres d'une stratégie nationale en matière de sécurité des réseaux et des systèmes d'information* définissant des objectifs stratégiques et les mesures politiques et réglementaires appropriées. Les Etats membres devront désigner une autorité nationale compétente pour la mise en œuvre de la directive ainsi que des centres de réponse aux incidents de sécurité informatique (CSIRT) ;

- *Le renforcement de la coopération et de l'échange d'informations entre les Etats membres* par la mise en place d'un groupe de coopération et la mise en réseau des CSIRT ;

- *L'imposition de mesures de sécurité appropriées aux opérateurs fournissant des services essentiels.* Ces opérateurs seront également tenus de notifier les incidents graves aux autorités nationales compétentes. Les secteurs concernés sont l'énergie, les transports, les services bancaires, les infrastructures de marchés financiers, la santé, l'eau et les infrastructures numériques. Les Etats membres seront chargés d'identifier les opérateurs concernés selon des critères définis par la directive.

Enfin, des exigences harmonisées seront applicables aux fournisseurs de services numériques, qui seront tenus de prendre des mesures de sécurité appropriées et de notifier à l'autorité compétente tout incident ayant un impact significatif sur la fourniture de services. Les fournisseurs concernés sont les marchés en ligne, les services de cloud computing et les moteurs de recherche.

La directive "Cybersécurité" est entrée en vigueur le 8 août 2016 et doit être transposée dans les droits nationaux avant le 9 mai 2018. A noter que les dispositions de cette directive rappellent celles imposées aux opérateurs d'importance vitale (OIV) par la loi de programmation militaire française 2014-2019 du 18 décembre 2013 (LPM), et ses premiers décrets d'application. (*Directive (UE) 2016/1148 du Parlement européen et du Conseil, du 6 juillet 2016 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union et voir notre [article de mai 2015](#) sur ce sujet*)

DROIT DES AFFAIRES

JURISPRUDENCE

Droit des contrats - La rupture, même prévisible, d'une relation commerciale établie, est brutale en l'absence de préavis écrit

Dans un arrêt du 6 septembre 2016, la Cour de cassation a décidé que, bien que prévisible, la rupture d'une relation commerciale établie peut être brutale si elle ne résulte pas d'un préavis écrit de résiliation.

En l'espèce, la société Sniw, qui exploite une centrale d'achats de produits alimentaires, approvisionnait la société US import export depuis 2003. En mars 2010, US import export a cessé de passer commande auprès de Sniw, du jour au lendemain, sans lui adresser ni lettre de rupture, ni préavis écrit. S'estimant victime de la rupture brutale d'une relation commerciale établie, la société Sniw a assigné la société US import export en réparation de son préjudice.

Selon la Cour, "le caractère prévisible de la rupture d'une relation commerciale établie ne prive pas celle-ci de son caractère brutal si elle ne résulte pas d'un acte du partenaire manifestant son intention de ne pas poursuivre la relation commerciale et faisant courir un délai de préavis (...)."

La Cour de cassation a donc confirmé l'arrêt de la Cour d'appel de Paris du 12 juin 2014 qui avait retenu la responsabilité de la société US import export. (*Cass. com., 6 sept. 2016, n°14-25.891, US import export c. Sniw ; et autres*)

DROIT FISCAL ET E-COMMERCE

RÉGLEMENTATION

Internet – Nouvelles obligations déclaratives à la charge des plateformes de mise en relation par voie électronique

La loi de finances pour 2016 instaure de nouvelles obligations déclaratives à la charge des plateformes de vente en ligne, depuis le 1er juillet 2016. Ces obligations s'appliquent aux sites de mise en relation entre acheteurs et vendeurs, à savoir les sites permettant la vente d'un bien, la fourniture d'un service ou l'échange ou partage d'un bien ou d'un service, tels que Leboncoin, Airbnb, Uber ou Blablacar par exemple.

Bien que les revenus issus de ces activités soient en principe soumis à l'impôt sur le revenu, les vendeurs déclarent très rarement.

Ces nouvelles obligations se déclinent de la manière suivante :

1 - Les plateformes devront d'une part fournir une information "loyale, claire et transparente" concernant les obligations fiscales et sociales qui incombent aux utilisateurs lors de chaque transaction réalisée par l'intermédiaire du site. Ces informations sont par ailleurs disponibles sur le site de l'administration fiscale. Un lien vers les sites des administrations devra figurer sur la plateforme afin de permettre aux vendeurs de se conformer à leurs obligations.

2 - Chaque année, au mois de janvier, les plateformes devront adresser aux vendeurs un document récapitulant le montant brut des transactions qu'ils ont perçu, par leur intermédiaire, au cours de l'année précédente, dont elles ont connaissance.

3 - Enfin, avant le 15 mars de chaque année (la première fois, le 15 mars 2017), les plateformes devront faire certifier par un tiers indépendant le respect des obligations susvisées (information des utilisateurs et envoi des documents récapitulatifs) et communiquer ce certificat par voie électronique à l'administration fiscale. L'absence de communication de ce certificat est passible d'une amende de 10.000 euros, sauf si l'exploitant de la plateforme envoie le certificat dans un délai de 30 jours.

Ces obligations s'appliquent d'une part aux entreprises, quel que soit le lieu de leur établissement, qui exploitent un site à destination du marché français, d'autre part aux utilisateurs résidant en France ou qui réalisent des ventes ou des prestations de services en France. (CGI, articles 242 bis et 1731 ter. ; LPF, articles L.102 AD et L.80 P)

VIE DU CABINET

SITE WEB DU CABINET

Le [site web du cabinet](#) connaît une nouvelle jeunesse ! La nouvelle version est en ligne depuis quelques jours.

PUBLICATIONS ET PRÉSENTATIONS

Vous trouverez sur le [Blog du Cabinet](#) toutes nos dernières publications :

- Adoption du Règlement européen sur la protection des données : le compte à rebours de la mise en conformité a commencé
- Nouvelle convention fiscale de non double imposition entre la France et Singapour : les conditions de retenue à la source pour les prestations de services
- Transferts de données personnelles vers les Etats-Unis : un bouclier de protection de données pour remplacer la sphère de sécurité

Nos dernières publications sur notre [Blog en anglais](#) :

- New double tax convention between Singapore and France: when does the withholding tax apply to French companies for services performed in Singapore?
- New European General Data Protection Regulation (GDPR): the compliance clock is ticking

Directeur de la publication : Bénédicte DELEPORTE

Editeur : DELEPORTE WENTZ AVOCAT - 5, rue Tronchet – 75008 Paris - Tel 01.40.17.95.86

Cette Lettre est une publication périodique diffusée gratuitement auprès d'un nombre limité de personnes ayant une relation directe ou indirecte avec le Cabinet. La Lettre ne saurait constituer ou être interprétée comme un acte de conseil juridique.

Le destinataire est seul responsable de l'usage qu'il fait des informations fournies dans la Lettre.