ALTANA
AVOCATS • PARIS

NEWSLETTER IP/IT

SEPTEMBRE 2016

A LA UNE :

DONNEES PERSONNELLES : AVEZ-VOUS ANTICIPE LES CHANGEMENTS ?

L'Union Européenne (ci-après « UE») a adopté le 14 avril 2016 un nouveau **Règlement** relatif à la protection des personnes physiques à l'égard **du traitement des données à caractère personnel** et à la libre circulation de ces données (Règlement (UE) 2016/679). Il entrera en vigueur en France à compter du **25 mai 2018.**

Afin d'anticiper au mieux l'entrée en vigueur de ce Règlement, en voici les principales nouveautés.

Champ d'application territorial

Le Règlement trouvera à s'appliquer notamment en fonction **(i) du lieu d'établissement** au sein de l'UE du responsable de traitement ou du sous-traitant, que le traitement ait lieu ou non dans l'Union, ou **(ii)** de **la situation de la personne** dont les données sont collectées (en zone UE ou hors zone UE) **et des activités liées au traitement** (à l'offre de biens ou de services à ces personnes concernées dans l'Union ou au suivi du comportement de ces personnes, dans la mesure où il s'agit d'un comportement qui a lieu au sein de l'Union).

Privacy by design et *Privacy by default*

Le responsable de traitement devra adopter des règles internes et des mesures techniques et organisationnelles qui respecteront le **principe de la protection** des données personnelles **dès la conception** (d'un service, d'un logiciel, etc.) (***Privacy by design***). Il s'agit par exemple de pseudonymiser les données dès que possible ; de garantir la transparence ; de permettre à la personne concernée de contrôler le traitement des données.

Ces mesures doivent également respecter le principe de la **protection des données personnelles par défaut** (***Privacy by default***) afin de garantir que seules les données nécessaires au regard de chaque finalité sont traitées, en laissant la possibilité à l'utilisateur d'élargir les paramètres par la suite.

Accountability ou l'obligation de rendre des comptes

Le responsable de traitement devra mettre en place des mécanismes et des procédures internes permettant **de démontrer et justifier du respect des règles relatives à la protection des données.**

L'objectif est d'identifier et de documenter les mesures mise en œuvre par le responsable de traitement, pour se conformer aux exigences issues du Règlement (tenue d'un registre, réalisation d'analyses d'impact, etc.).

Cette **obligation de documentation** aura des conséquences pratiques considérables pour les entreprises qui devront l'intégrer à leurs procédures internes, sensibiliser et former les différents services, et centraliser l'information auprès d'une personne dédiée.

L'autorité de contrôle pourra vérifier le respect de ces obligations en tout temps. Les entreprises **auront l'obligation de notifier** à l'autorité de contrôle toute violation au traitement de données dans les meilleurs délais (maximum 72h) ainsi qu'aux personnes concernées.

Profilage

Le Règlement **formalise cette notion** qu'il définit comme une forme de traitement automatisé particulière permettant d'utiliser ces données à caractère personnel pour évaluer certains aspects personnels à une personne physique (santé, intérêts, localisation, etc.).

Le profilage ne pourra se faire sans le consentement de la personne concernée. Cette dernière devra pouvoir s'opposer à tout

moment à son profilage. Ce droit devra être explicitement porté à l'attention de la personne concernée et présenté clairement et séparément de toute autre information.

Responsabilité nouvelle du sous-traitant

Le Règlement instaure un **principe de responsabilité des sous-traitants**.

Les **sous-traitants auront désormais des obligations propres et des obligations partagées** avec le responsable de traitement. Cette responsabilité sera solidaire entre les deux acteurs à l'égard de la personne concernée, lorsqu'ils participent à un même traitement. Cela permet de garantir à la personne concernée une réparation effective.

Outre la responsabilité à l'égard de la personne concernée, la CNIL pourra également s'adresser directement au sous-traitant, contrôler son activité, et le cas échéant, le sanctionner.

Renforcement de l'obligation d'information

En plus des informations devant déjà être fournies par le responsable de traitement en application du régime actuel, celui-ci **devra informer la personne concernée** notamment de son droit d'introduire une réclamation auprès d'une autorité de contrôle, de l'existence de prise de décision automatisée (dont le profilage), des coordonnées du délégué à la protection des données éventuellement désigné, de la source des données lorsque celles-ci n'ont pas été collectées directement auprès de la personne concernée, etc.

Ce renforcement aura pour conséquence pratique pour les entreprises **de devoir réviser les politiques de confidentialité** et autres documents vecteurs de cette information, sur lesquels il est aujourd'hui fait référence au droit d'accès et de rectification.

Obligation de désigner un délégué à la protection des données

La désignation d'un « correspondant informatique et libertés » ou « CIL » selon la terminologie de la loi du 6 janvier 1978 est aujourd'hui une faculté accordée aux responsables de traitement.

Le Règlement érige la **désignation d'un « délégué à la protection des données » ou « DPO » en obligation** dans certains cas.

Ainsi, seront notamment obligés de désigner un DPO, les responsables de traitement ou sous-traitants dont les activités de base consistent en des opérations de traitement qui, du fait de leur nature, de leur portée et/ou de leurs finalités, exigent un suivi régulier et systématique à grande échelle des personnes concernées.

Les entreprises devront alors déterminer si la nature de leurs activités entre dans le champ de cette définition, et si, par conséquent, elles sont soumises à cette nouvelle obligation.

Sanctions

Le Règlement prévoit une **hausse considérable des pouvoirs de sanctions pécuniaires de la CNIL.** Celles-ci pourront aller jusqu'à 20 millions d'euros et 4% du chiffre d'affaires de l'entreprise.

Le projet de loi pour une République Numérique (« Loi Lemaire ») a commencé à **anticiper cette hausse des sanctions** de la CNIL en augmentant le plafond de 150 000 euros à 3 millions d'euros. Cette loi devrait être adoptée au cours du 2ème semestre 2016.

Pour approfondir

Altana organisera prochainement un **petit-déjeuner** sur le **thème de la Cybersécurité** où ces points seront développés, sous un angle pratique.

ACTUALITES JURISPRUDENTIELLES

Encadrement des clauses de « loi applicable » dans les CGV de e-commerce

La Cour de Justice de l'Union Européenne (ci-après « CJUE ») a été saisie d'une question préjudicielle visant à savoir si une clause figurant dans des conditions générales d'un contrat de e-commerce entre un consommateur et un professionnel, qui applique au contrat uniquement la loi du pays où est établi le professionnel est **abusive ou non.**

La Cour a répondu à cette question en retenant qu'une telle clause peut être abusive, **lorsqu'elle induit le consommateur en erreur, en lui donnant l'impression que seule la loi de cet Etat Membre s'applique**, sans l'informer de ce qu'il

bénéficie également de la protection du droit qui lui serait applicable en l'absence de cette clause.

Cette solution fait écho à l'arrêt de la Cour d'appel de Paris du 12 février 2016, qui a qualifié d'abusive la **clause attributive de juridiction** insérée dans les conditions générales de Facebook.
L'attribution de compétence aux tribunaux de Californie, engendrait en effet, selon la Cour, des difficultés pratiques et un coût d'accès aux juridictions de nature à dissuader le consommateur d'exercer toute action.

CJUE – 28 juillet 2016, C-191/15 *Verein für Konsumenteninformation / Amazon EU SARL*

La communication sur une décision de justice qui concerne un concurrent

Deux décisions ont été rendues concernant les possibilités d'une entreprise de communiquer sur un jugement qui condamne un concurrent.

La Cour d'appel de Paris a considéré que **l'envoi par email à des clients et prospects** par une société **d'un jugement non-définitif rendu à l'égard d'un concurrent** ne suffit pas à constituer un acte de **dénigrement et de concurrence déloyale.**
La seule communication d'une décision de justice, qui est par essence publique, n'est pas constitutive d'un acte de dénigrement.

A l'inverse, le Tribunal de commerce de Lyon a estimé qu'une société qui a communiqué à un prospect **une décision de justice tronquée et erronée** concernant un concurrent, commet un acte de dénigrement.

CA Paris, Pôle 1, Ch. 2 - 16 juin 2016
Tribunal de commerce de Lyon – 22 juin 2016

Responsabilité des places de marché physiques en tant qu'intermédiaires

Par un arrêt du 7 juillet 2016, la CJUE a considéré **qu'une société qui sous-loue des emplacements** dans des halles de marchés, où sont vendues des contrefaçons doit être considéré comme un **intermédiaire** au sens de la directive 2004/48.

La notion d'intermédiaire peut donc s'appliquer aux exploitants de places de marchés en ligne comme physiques.

L'intermédiaire peut être contraint par **injonction de prendre certaines mesures visant à faire cesser les faits de contrefaçon** (faciliter l'identification du vendeur, suspendre l'auteur de l'atteinte à des droits de propriété intellectuelle pour éviter que de nouvelles atteintes de cette nature par le même commerçant aux mêmes marques aient lieu, etc.).

La Cour précise cependant que l'intermédiaire ne peut pas être soumis à une obligation de **surveillance générale** et permanente, car une telle injonction serait excessivement coûteuse et créerait un obstacle au commerce légitime.

CJUE – 7 juillet 2016, C-494/15 *Tommy Hilfiger Licensing e.a.*

Absence de protection contre l'imitation d'une enseigne insuffisamment distinctive

Un ancien franchisé « Optical Center » a cédé son fonds de commerce. Le cessionnaire l'exploite depuis sous l'enseigne « Optical Centre ».

La société Optical Center, qui utilise ce nom comme enseigne, a assigné ce dernier, considérant qu'il portait atteinte à son enseigne et qu'il existait un risque de confusion entre les deux.

Malgré la ressemblance pouvant exister entre les termes, la Cour d'appel de Paris a refusé d'accéder aux demandes d'Optical Center, **considérant que l'enseigne en cause n'était pas suffisamment distinctive**, et qu'en ce qu'elle ne permettait pas d'identifier une origine commerciale, il n'existait pas de risque de confusion.

Optical Center considérait également que le magasin imitait **l'agencement des magasins** conçu par le réseau de franchise. Ce grief a été également écarté par la Cour, qui a considéré que l'agencement en cause était banal, car commandé par la nature de l'activité.

CA Paris, Pôle 5, Ch.1 – 24 mai 2016

EN BREF

Le 12 juillet 2016, la Commission Européenne a **adopté** la décision d'adéquation du **Privacy Shield**. Ce texte, qui crée un nouveau **cadre** pour les **transferts** de données entre l'Union Européenne et **les Etats-Unis**, entrera en vigueur à compter de sa notification à chacun des Etats Membres. Il sera applicable aux entreprises qui se seront enregistrées auprès des autorités américaines en charge de la mise en œuvre du dispositif.

Dans une réponse ministérielle du 12 juillet 2016, la Secrétaire d'État chargée du Commerce, de l'Artisanat, de la Consommation et de l'Economie sociale et solidaire indique que les pratiques **d'*IP tracking***, permettant aux sites de e-commerce de moduler les prix en fonction du comportement de l'internaute, pourraient être appréhendées comme une pratique **commerciale déloyale et trompeuse**, et/ou sur le fondement de la règlementation des **données personnelles.**

LE COIN DU PRATICIEN :

PROTEGER LES SECRETS DES AFFAIRES DE L'ENTREPRISE

Après le retrait, en février 2015, des dispositions du projet de « Loi Macron » portant sur la protection des secrets des affaires, l'Union Européenne a adopté un texte permettant une **protection spéciale et harmonisée** de ces secrets.

La Directive n° 2016/943 sur la protection des savoir-faire et des informations commerciales non divulgués (secrets d'affaires) contre l'obtention, l'utilisation et la divulgation illicites (la « ***Directive secret des affaires*** ») du 8 juin 2016, est entrée en vigueur le **5 juillet dernier**.

Principales dispositions de la Directive secret des affaires

La Directive secret des affaires prévoit notamment :

- Une **définition** des notions de « secrets d'affaires », et de leur obtention, utilisation et divulgation licites et illicites ;
- Des **exceptions** afin, notamment, d'assurer la **liberté d'expression et d'information**, et de protéger les « **lanceurs d'alerte** » agissant dans un but d'intérêt général ;
- Dans le cadre de **procédures judiciaires**, une obligation de confidentialité, notamment à la charge des parties et du personnel judiciaire, permettant **de préserver le secret.** Sauf exception, la confidentialité devra être respectée **même après le terme** de la procédure.
- Des types **d'injonctions et de mesures coercitive**s pouvant être ordonnées à l'encontre d'un contrevenant ;
- Des règles de **fixation des dommages et intérêts** pouvant être accordés à une entreprise lésée.

Les moyens actuels de protections des secrets des affaires

Un délai de deux ans est prévu pour procéder à la transposition de la Directive – soit le **9 juin 2018.**

Dans l'intervalle, le droit positif offre tout de même aux entreprises différents moyens de protéger leurs secrets des affaires.

En effet, le droit pénal réprime par exemple le **vol d'information**, l'abus de confiance, ou le fait pour un salarié de révéler un secret de fabrication.

La responsabilité civile délictuelle peut également être engagée, **sur le fondement de la concurrence déloyale**.

Il faut noter à cet égard que la récente réforme du droit des contrats prévoit une obligation **légale de confidentialité** des informations obtenues dans le cadre de **négociations**.

Il est également possible de stipuler des clauses de confidentialité, dans les **contrats de travail des salariés** ainsi que dans les contrats conclus avec des tiers (prestataires, fournisseurs, etc.).

La prévision contractuelle d'une telle obligation permet notamment de définir précisément le champ des informations couvertes par la confidentialité.

Mesures préventives

Certaines **mesures organisationnelles et techniques** peuvent être prises par les entreprises afin de **prévenir une atteinte** à leurs secrets des affaires.

Les entreprises peuvent **classifier leurs données en fonction de leur sensibilité** et adopter des mesures techniques de protection correspondantes.

Les informations confidentielles doivent être **clairement identifiées comme telles,** notamment par les personnes qui les utilisent, en apposant par exemple la mention « confidentiel » sur les documents ou lors d'envoi d'emails.

L'attention doit également être importante lors du **départ d'un salarié** ou d'un changement de prestataire, et des moyens techniques doivent permettre un contrôle de l'employeur. Ces mesures doivent pour autant respecter des dispositions du droit du travail et de protection de la **vie privée des salariés**.

VIE DU CABINET

L'équipe IP-IT, en collaboration avec l'équipe Pénal, organisera en novembre un petit-déjeuner sur le **thème de la Cybersécurité.**

Le Cabinet a le plaisir de vous informer de l'arrivée de **Marie Hindré, en qualité d'Associée**, qui vient renforcer **le Pôle Droit Economique et de la Concurrence**. Nous lui souhaitons la bienvenue parmi nous.

ALTANA
VOCATS • PARIS

45 rue de Tocqueville • 75017 Paris, France
Tél. : +33 (0)1 79 97 93 00
www.altanalaw.com

L'équipe IP /IT d'Altana

Pierre Lubet / **plubet@altanalaw.com**
Jean-Guy de Ruffray / **jgderuffray@altanalaw.com**
Camille Raclet / **craclet@altanalaw.com**