IT LAW Avocats

PROTECTION DES DONNEES PERSONNELLES

Vers une clarification des procédures de contrôle et de sanction de la CNIL

L'année 2011 s'est achevée avec l'adoption tant attendue du décret[1] relatif aux pouvoirs de contrôle et de sanction de la Commission nationale de l'informatique et des libertés (CNIL). Ce dernier vient modifier le décret du 20 octobre 2005.

En effet, depuis 2004 la CNIL dispose de moyens d'actions coercitifs afin de s'assurer du respect des dispositions de la loi du 6 janvier 1978. Cependant, les pouvoirs de la CNIL en matière de contrôle ont été fortement remis en cause à la suite de deux décisions du Conseil d'Etat de 2009 annulant des procédures jugées excessives au regard de l'article 8 de la CESDH relatif au droit au respect du domicile et de la vie privée.

Ces décisions ont appelé le législateur à réviser les règles encadrant ces procédures.

1. Réforme du contrôle sur place

A la suite des décisions du Conseil d'Etat, risquant de freiner l'action de la CNIL, une loi insérant des garanties supplémentaires a été adoptée le 29 mars 2011, afin d'encadrer d'avantage la procédure de contrôle de la CNIL.
Le décret du 29 décembre 2011 vient en préciser les conditions d'applications.

Le texte pose les conditions :

- d'information du responsable des lieux (représentant de l'entité subissant le contrôle) quant à la visite des agents de la CNIL a des fins de contrôle. Notamment, l'information de cette visite doit intervenir au plus tard au moment de l'arrivée sur place des agents. Par ailleurs, il doit être fait mention du droit d'opposition dont dispose le responsable des lieux audit contrôle. Les motifs de cette opposition seront portés au procès-verbal dressé par les agents de la CNIL.
- En cas d'opposition, la visite ne pourra être effectuée qu'après l'autorisation du juge des libertés et de la détention qui dispose de 48h pour accepter ou refuser la demande d'autorisation transmise par la CNIL pour assurer la visite auprès. A ce titre, le décret fixe notamment ce que doit contenir l'acte de notification (mention et délais des voies de recours et possibilité de demandé la suspension ou l'arrêt de la visite) de l'ordonnance rendue par le juge.
- Cette ordonnance est susceptible de recours devant le premier Président de la Cour d'appel.

Enfin, le juge des libertés et de la détention peut, s'il l'estime utile, se rendre sur place à l'occasion de la visite, et décider à tout moment de sa suspension ou de son arrêt.

2. Les procédures devant la formation restreinte et les sanctions prononcées

Le nouveau décret organise par ailleurs la procédure applicable devant la formation restreinte de la CNIL (Formation contentieuse composée du président et de cinq autres membres élus par la commission en son sein) et précise le déroulement de ses séances.

Parmi les nouveautés, les mises en demeure adressées aux responsables de traitement par la CNIL en cas de manquements à leurs obligations au regard de la loi de 1978, sont désormais décidées par le Président de la CNIL, alors qu'elles l'étaient auparavant par la formation restreinte.

[1] Décret n° 2011-2023 du 29 décembre 2011 relatif aux pouvoirs de contrôle et de sanction de la Commission nationale de l'informatique et des libertés

Ces mises en demeure doivent mentionner les délais dans lesquels le responsable d'un traitement de données à caractère personnel est tenu de se conformer à la loi et de mettre fin aux manquements constatés par la CNIL. Ce délai peut être renouvelé une fois si la complexité de l'affaire le justifie.

En cas de contrôle de la CNIL il est vivement conseillé :

- Pendant le contrôle :
  - de vérifier que l'information de la visite de la CNIL est conforme au décret et notamment qu'elle mentionne : votre droit d'opposition et les voies de recours
  - de faire en sorte que les contrôleurs de la CNIL ne sortent pas du périmètre du contrôle qui leur est défini
  - de relire soigneusement le procès-verbal établi à la fin du contrôle afin de demander toute modification / précision utile surtout sur les procédés techniques contrôlés
  - de faire inscrire toute observation et réserve utile
- Après le contrôle :
  - prévoir de mettre en place un audit CNIL pour identifier les actions de mise en conformité à la règlementation informatique et liberté
  - dès réception de la mise en demeure de la CNIL qui suivra le contrôle : mettre en conformité les points identifiés dans cette mise en demeure.

IT LAW Avocats

PROTECTION DES DONNEES PERSONNELLES

Prospection par SMS : veillez au consentement des personnes !

La Commission Nationale de l'Informatique et des Libertés a prononcé le 12 janvier dernier une sanction pécuniaire de 20 000 euros à l'encontre du groupe D.S.E. France et a rappelé que **l'envoi de publicité commerciale par voie électronique ne peut pas intervenir sans l'accord préalable du destinataire.**

A l'origine de cette délibération :

- L'envoi de centaines de milliers de SMS, sans leur consentement, à des particuliers proposant à la vente leur bien immobilier sur internet, par une société qui leur proposait des bilans diagnostic de leurs biens immobiliers ;

- L'absence de prise en compte par cette société des demandes des particuliers exigeant que l'envoi de SMS non désirés cesse ;

Les données des particuliers, et notamment leurs numéros de téléphone, étaient collectées par des sociétés spécialisées dans l'aspiration de données sur Internet. Celles-ci collectaient les données figurant dans les annonces immobilières en ligne, puis constituaient un fichier pour le revendre au groupe D.S.E qui l'utilisait aux fins de démarchage par SMS.

Plusieurs personnes ainsi démarchées avaient vainement tenté de s'opposer à ces SMS et en désespoir de cause avaient saisi la CNIL en déposant plainte.

Cette pratique du groupe D.S.E France portait en effet atteinte aux obligations suivantes :

- Obtenir le consentement préalable à tout démarchage par SMS

- Informer les personnes concernées par la collecte[2] : mention de l'identité de l'organisme à l'origine de la collecte, de la finalité de cette collecte ainsi que de leurs droits à accéder, rectifier, supprimer les informations les concernant ou encore de s'opposer à leur collecte[3]. En l'espèce, les SMS envoyés par la société ne contenaient aucune de ces mentions d'information, ni aucun renvoi vers un site Internet sur lequel la personne concernée aurait pu les consulter.

- Assurer le droit d'opposition : toute personne concernée par la collecte doit pouvoir s'opposer à ce que ses données soient traitées et conservées. Dans notre espèce, outre l'absence d'information des particuliers quant à leur droit d'opposition, celui-ci n'était même pas respecté. Il aurait en effet été préférable que le groupe D.S.E France satisfasse aux demandes d'opposition des particuliers exigeant la cessation des envois de SMS.

La CNIL a donc prononcé à l'encontre du groupe D.S.E France une sanction pécuniaire de 20 000 € et a ordonné la publication de la délibération sur le site Internet de la CNIL et sur Légifrance.

Il s'agit là de la première décision prise à l'encontre d'un organisme utilisant les fichiers créés par des sociétés qui « aspirent » des données pour démarcher de nouveaux clients.

Mais prudence car ce ne sera probablement pas la dernière ; outre le fait qu'elles « spament » les personnes, ces pratiques faussent le jeu de la concurrence entre les sociétés proposant les même services.

Nul doute que la CNIL soit déterminée à faire cesser ce genre de pratiques !

[2] Article 32 Loi Informatique et Libertés du 6 janvier 1978
[3] Article 38 Loi Informatique et Libertés du 6 janvier 1978

IT LAW Avocats

PROTECTION DES DONNEES PERSONNELLES

La CNIL sanctionne un système de vidéosurveillance pour les salariés

A la suite d'une plainte d'un salarié, la CNIL a procédé au contrôle le 12 octobre 2011 du système de vidéosurveillance installé par une société dans ses locaux.

Les agents de la CNIL ont ainsi pu constater que 8 caméras avaient été installées et que celles-ci comprenaient également des microphones.

Ce dispositif de vidéosurveillance avait fait l'objet d'une déclaration auprès de la CNIL et la finalité ainsi déclarée était : "*sécurité des biens et des personnes*".

Cependant à la lecture des avertissements adressés par la société aux salariés, il semble que la finalité ait été autre dans la réalité. En effet, deux salariés se sont vus reprochés les faits suivants : "*A de nombreuses reprises il vous a été demandé de cesser de mâcher votre chewing-gum et d'arrêter de faire claquer des bulles*"

Outre le détournement de finalité, les agents ont constaté que la durée de conservation des données n'était pas respectée puisque ces derniers pouvaient remonter jusqu'à 4 mois. Rappelons qu'en matière de vidéosurveillance la durée maximale de conservation est d'un mois.

La CNIL a donc mis en demeure la société de se mettre en conformité avec la règlementation informatique et libertés et notamment de :

- mettre fin au dispositif audio des caméras,
- respecter la durée de conservation maximale de 1 mois,
- veiller au respect de la finalité, à l'adéquation, à la pertinence et au caractère non excessif du traitement et donc d'éviter que les salariés soient filmés en permanence.

La CNIL a également décidé la publication de cette mise en demeure sur le site internet de la CNIL.

Compte tenu de cette décision de la CNIL, nous recommandons en particulier de :

- vérifier que l'utilisation des dispositifs de vidéosurveillance est en corrélation avec la finalité déclarée auprès de la CNIL et bien entendu que cette finalité déclarée n'est pas « excessive ».
- s'assurer du respect des durées de conservation des données : un mois pour la vidéosurveillance par exemple.
- renforcer l'information des personnes concernées comme les salariés en intégrant de tels dispositifs d'information dans les contrats de travail ou le règlement d'entreprise sans oublier l'affichage.
- mettre en place une Charte informatique afin de sensibiliser d'avantage les personnes chargées de la mise en œuvre d'un traitement ou disposant d'un accès.

IT LAW Avocats

PROTECTION DES DONNEES PERSONNELLES

Données à caractère personnel: Vers la fin des disparités entre les législations européennes ?

Le 25 janvier 2012, la Commission européenne a proposé une réforme des règles de protection des données à caractère personnel qui avaient été introduites par la directive européenne du 24 octobre 1995.

Cette proposition de réforme est constituée :

- d'une *proposition de règlement qui définit un cadre général de protection des données à caractère personnel dans l'Union européenne*.
- d'une *proposition de directive relative à la protection des données à caractère personnel traitées à des fins de de prévention et de détention des infractions pénales, d'enquêtes et de poursuite en la matière ainsi que l'activités judiciaires connexes*

Dans le contexte actuel d'accroissement des traitements de données à caractère personnel et d'internationalisation de leurs échanges, cette initiative de la Commission européenne a pour objectif de renforcer l'harmonisation et la simplification des règles applicables dans ce domaine afin d'assurer un équilibre entre une protection adéquate de la vie privée des personnes et la libre circulation des données à caractère personnel au sein de l'Union Européenne.

Il est notamment proposé :

- un droit à l'oubli numérique qui permettrait aux personnes concernées d'obtenir du responsable de traitement la suppression des données les concernant ainsi que l'effacement de tout lien vers ces données ou les copies ou reproductions qui en ont été faites, si aucun motif légitime ne justifie leur conservation. Aujourd'hui en vertu de la Loi Informatique et Libertés, seul un droit d'opposition est reconnu au bénéfice des personnes concernées ;
- un droit à la portabilité des données dont l'objectif est de faciliter *« l'accès des personnes concernées à leurs données »* ainsi que *« le transfert de données à caractère personnel d'un prestataire de service à un autre »* ;
- le renforcement des règles de recueil des consentements. Par exemple, dans tous les cas où le consentement des personnes concernées est nécessaire pour procéder au traitement des données, le consentement devra être exprès.
- l'obligation pour le responsable de traitement de nommer *« un délégué à la protection des données »* lorsque (i) *« le traitement est effectué par une autorité ou un organisme public »* (ii) *« le traitement est effectué par une entreprise employant 250 personnes ou plus »* ou (iii) les traitements qui de par leur nature, portée et/ou finalités nécessitent un suivi régulier et systématique des personnes concernées;

- le renforcement des sanctions à l'égard des entités ne respectant pas ces règles. A titre d'exemple, les autorités nationales indépendantes chargées de la protection des données à caractère personnel seront habilitées à infliger aux entités contrevenantes des amendes pouvant atteindre un million d'euros ou 2% de leur chiffre d'affaire global ;

- l'introduction du critère de l'établissement principal du responsable de traitement pour déterminer l'autorité compétente pour connaître des traitements mis en œuvre sur le territoire de l'Union, pour se prononcer sur les plaintes et/ou l'exercice des droits qui sont reconnus aux personnes concernées ;

- la concentration des pouvoirs entre les mains de la Commission européenne en matière de protection des données à caractère personnel.

Si l'initiative et les objectifs généraux de ces propositions ont été salués, en France, des réserves ont néanmoins été formulées à l'égard de certaines de ces mesures.

Ainsi par exemple le critère de l'établissement principal, perçu comme une perte de proximité avec les citoyens et favorisant la pratique de « forum shopping », est vivement contesté. De même, le pouvoir accordé à la Commission qui sera compétente pour déterminer les lignes directrices en matière de protection des données à caractère personnel, au détriment des autorités nationales ainsi que la possibilité offerte pour le seul responsable de traitement de déterminer la pertinence de transferts de certaines données, sont dénoncés.

Cette proposition de règlement et de directive a été soumise au Conseil de l'Union européenne et au Parlement européen pour être examinée et adoptée.

Rappelons que le règlement, une fois adopté, sera d'application immédiate dans l'ensemble des Etats membres de l'Union européenne sans qu'aucune transposition ne soit nécessaire.

Nous ne manquerons pas de vous tenir informés de son évolution.

3 questions = 1 conseil

Bases de données : comment les utiliser ?

L'entreprise ne peut pas utiliser comme bon lui semble les données personnelles trouvées sur le net ou ses bases de données clients. Malgré l'évolution des technologies, la protection des données à caractère personnel s'impose.

Peut-on envoyer des offres de services aux prospects dont on trouve les coordonnées sur les réseaux sociaux ou dans des annuaires ?

Non, pour utiliser des données collectées *via* des supports tels que les réseaux sociaux ou des annuaires, il faut avoir, au préalable, obtenu l'accord de la personne concernée et aussi l'avoir informé de son droit d'opposition.

Cet accord peut être obtenu si, lors de l'inscription de ses coordonnées sur le site du réseau social ou dans l'annuaire, la personne concernée a été informée que les données collectées pourraient faire l'objet d'un transfert à des tiers à des fins commerciales et qu'elle a expressément donné son accord pour un telle utilisation.

Peut-on vendre sa base de données clients ?

Non. Les cessions de fichier sont autorisées à condition que les personnes concernées aient été prévenues de cette éventualité et aient accepté le principe.

Il convient donc aussi ici, au préalable, d'informer les personnes concernées de ces transferts de données à des tiers, de préciser les finalités de ces transferts (à des fins de statistiques, commerciales...) et surtout d'obtenir leur consentement. Il est alors primordial de toujours permettre à la personne concernée de pouvoir s'opposer à ce que ses données soient transférées à des tiers.

Peut-on héberger sa base de données clients auprès de n'importe quel prestataire dans le monde ou en Cloud Computing ?

Oui si on respecte certaines conditions. La loi Informatique et libertés de 1978 (modifiée par la loi de 2004 transposant la directive du 24 octobre 1995) a, en effet, précisé les conditions de transfert de données à caractère personnel vers des pays n'assurant pas un niveau de protection adéquat au sens de la directive, c'est-à-dire à peu près l'ensemble des pays hors UE, y compris Monaco !

L'hébergement des données dans un pays dit « tiers », par une société à laquelle la loi française s'applique, doit donc être encadré par des clauses contractuelles types, ou selon les principes du *Safe Harbor* (pour un hébergement situé aux USA), ou sur la base de BCR (*Binding Corporate Rules*), ou selon une des exceptions de l'article 69 de la loi Informatique et libertés (sauvegarde de l'intérêt public, consentement de la personne...ceci demeurant des exceptions). Pour un hébergement sur des serveurs dans un pays tiers déterminé ou *via* le système du Cloud Computing, les transferts de données devront ainsi respecter ces modalités d'encadrement et être soumis à l'autorisation de la CNIL pour être conformes à la réglementation Informatique et libertés française et européenne. Si le Cloud Computing pose tant de soucis quant à la protection des données personnelles, c'est parce qu'il implique que le responsable de traitement perd en partie la maîtrise de la localisation de ses données.

NOTRE CONSEIL

► **A l'égard des personnes dont les données sont traitées** : les informer, obtenir leur consentement, surtout si les informations proviennent de tiers, et leur accorder les droits d'accès, de rectification et d'opposition
► **A l'égard des sous-traitants** (gérant, administrant ou hébergeant les données) : intégrer aux contrats les mesures de transferts, de sécurité, de confidentialité, d'intégrité et les responsabilités de chacun au regard de la loi Informatique et libertés
► **A l'égard des salariés** : les sensibiliser sur l'utilisation des outils informatiques et la protection des données personnelles via une Charte Informatique ou une Politique de confidentialité.

LE CHIFFRE DU MOIS

La Sécurité des entreprises :

78% des vulnérabilités se situent désormais dans les applications tierces (selon Secunia).

Il est donc important que les entreprises intègrent ce paramètre dans leur politique de sécurité en :

- en ne négligeant pas des logiciels moins critiques pour leur activité, mais fréquemment attaqués
- en mettant en place une véritable charte de sécurité pour sécuriser leur système d'information de l'intérieur de l'entreprise
- en intégrant dans leur contrat avec leurs éditeurs et prestataires les clauses de garantie et d'audit adaptées
- en mettant faisant ou en faisant faire des tests d'intrusion pour vérifier le niveau de sécurité tant de l'extérieur que de l'intérieur

LA PRESSE EN PARLE…

Notre premier article paru dans la presse …. C'était le 9 février 2012 … dans le nouvel économiste

Communiqué

ITLAW Avocats :
« La propriété intellectuelle, un capital à protéger »

Rencontre avec Claudia Weber, Avocat, fondatrice du cabinet ITLAW Avocats

Votre département Propriété intellectuelle constitue aujourd'hui un des piliers de votre Cabinet. Pourquoi ?

Car la propriété intellectuelle est devenue un domaine incontournable dans les projets à dominante technologique. Créer un site Internet, développer ou faire évoluer une application, mettre à disposition, stocker, louer, partager ou permettre à ses clients de télécharger ou consulter des œuvres intellectuelles (logiciel, photo, musique, vidéo, texte…), utiliser des logiciels open source, le cloud computing, nécessite de connaître les contraintes du droit de la propriété intellectuelle. Il est impératif d'assurer la protection et l'exploitation de son patrimoine intellectuel en conformité avec les lois applicables, d'autant que l'internationalisation complexifie encore davantage les schémas juridiques. Aussi, proposons-nous de larges prestations : audit, conseil, assistance juridique en entreprise, contrats, précontentieux, médiation, transaction, contentieux. Nous intervenons, par exemple, pour auditer des projets, identifier les contraintes légales et trouver des solutions, s'assurer que le client dispose bien des droits sur chacune des œuvres, valider la conformité des projets au droit de la propriété intellectuelle, puis mettre en place la protection juridique adaptée aux enjeux, élaborer et négocier les contrats nécessaires à l'utilisation et à l'exploitation des œuvres et enfin assister le client en cas de procédure, même si nous privilégions toujours la médiation au contentieux. Le respect des règles légales en matière de propriété intellectuelle permet d'anticiper les contentieux.

Votre spécialisation en droit des Nouvelles Technologies de l'Information et des Communications vous permet d'intervenir sur davantage de projets ?

Oui, c'est notre force. Nous intervenons tant dans le cadre des régimes de protection traditionnelle - droit d'auteur, marque, dessins et modèles, secret des affaires, concurrence déloyale - que des régimes de protection plus récents et spécifiques aux logiciels, noms de domaines, bases de données, œuvres multimédia ou audiovisuelles. Or, rares sont aujourd'hui les projets n'intégrant pas technologie et innovation ! Protéger un projet innovant nécessite ainsi d'identifier tous ses composants pour définir, composant par composant, les modes de protection adaptés, ce qui implique souvent de les cumuler. Nous proposons toujours des solutions concrètes, originales, adaptées à chaque projet, tenant compte des réalités opérationnelles, économiques et technologiques. Nous devons avoir à la fois une parfaite maîtrise du droit de la propriété intellectuelle, mais aussi savoir l'associer à la connaissance des technologies, faire preuve de grande rigueur et aussi de créativité et de veille constante : la complexité et l'évolution rapide des technologies et de leur cadre juridique constitue une vraie source d'insécurité pour les entreprises régulièrement confrontées à de nouveaux risques juridiques. Surtout en matière de projets innovants. Nous en informons régulièrement nos clients via nos formations et newsletters.

Si vous deviez donner un conseil, quel serait-il ?

Faire preuve de prudence et balayer les idées reçues. On oublie trop souvent, quand on confie la réalisation d'une œuvre intellectuelle à un prestataire - logiciel, site Internet (textes, photos, vidéos, charte graphique, logo, etc.) - que seul ce prestataire détient les droits de propriété intellectuelle, même si le client a payé la prestation et participé à la réalisation de l'œuvre, si aucun contrat de cession n'a été signé. Sans compter que, pour être valable, ce contrat doit encore répondre à des conditions légales bien strictes, de fond et de forme !

ITLAW Avocats
Propriété intellectuelle, Informatique, Internet, Télécoms, Informatique & Libertés
281 rue de Vaugirard 75015 Paris - Tél.: +33(0)1.83.62.61.75 - Mob. : +33(0)6.13.24.58.44
Fax : +33(0)1.83 .64.61.95 - Email de contact : claudia.weber@itlaw.fr
http://www.itlaw.fr
Twitter : twitter.com/ITLAWAvocats

ITLAW Avocats

EVENEMENT : « BPO : LEURRE OU ELDORADO ? »

Nous profitons de l'occasion de cette newsletter pour nous faire le relais d'un évènement qui nous tient à cœur : le **colloque Global RH qui se tient les 27, 28 et 29 mars prochains au Palais Brongniart Paris 2ème.**

Ce colloque a notamment pour objectif de rassembler les acteurs de la gestion RH et de créer un débat autour de grands thèmes d'actualité stratégiques dans ce domaine et notamment en lien avec l'évolution fulgurante de cette fonction.

A l'issue de ces trois jours de réflexion, vous pourrez également assister à la cérémonie de remise des Trophées des Binômes PDG/DRH.

Nous avons l'honneur et la chance de participer à ce colloque en association avec le groupe Althéa sur le thème « **BPO : LEURRE OU ELDORADO** », conférence-débat qui ayant lieu le 27 mars de 9h00 à 12h30

Pour toute information supplémentaire ou pour obtenir un carton d'inscription toute l'équipe d'ITLAW Avocats est à votre disposition.

Vous pouvez également vous rendre sur le site du groupe Althéa : http://www.althea-groupe.com/Acteur-tres-implique-dans-la-9eme.

En espérant vous y voir nombreux !

Claudia WEBER

Retrouvez nos articles sur *www.itlaw.fr*

Directeur de publication : Claudia Weber (claudia.weber@itlaw.fr)

IT LAW Avocats

281 rue de Vaugirard
75015 PARIS
Tél : 01 83 62 61 75
Fax : 01 83 64 61 95