LEXING ALAIN BENSOUSSAN
Juristendances Informatique et Libertés
n° 56-Mars-Avril-2014

LUTTE CONTRE LA SURVEILLANCE MASSIVE DES CITOYENS : LES SUITES DE L'AFFAIRE PRISM

Protection des données et de la vie privée des citoyens européens

▪ Les autorités européennes ont commencé à prendre des mesures suite à l'affaire Prism relative au programme de surveillance mis en place par les Etats-Unis permettant à la NSA (National Security Agency – l'agence nationale de sécurité américaine) de collecter les communications électroniques mondiales échangées sur les services en ligne.
▪ Ces activités de surveillance massive ont provoqué un débat international sur les conséquences de ces pratiques sur la vie privée des citoyens. En effet, si la lutte contre le terrorisme ou certaines menaces à l'ordre public peuvent justifier des atteintes ponctuelles et ciblées à la vie privée des personnes, cela ne pourrait justifier une surveillance généralisée et indifférenciée de la population.
▪ Dans le cadre du projet de règlement européen pour la protection des données à caractère personnel, le Parlement européen a proposé l'introduction d'un contrôle préalable des autorités de protection sur les demandes d'accès aux données relatives à des citoyens européens adressées à des entreprises par des autorités administratives et judiciaires de pays tiers (1).
▪ Ainsi, avant de communiquer les données personnelles de citoyens européens à un pays tiers, toute entreprise (par exemple, un moteur de recherche, un réseau social ou un fournisseur de services d'informatique en nuage) serait tenue de demander une autorisation préalable à une autorité nationale de protection des données dans l'Union européenne. Les entreprises devraient également informer la personne concernée d'une telle demande.
▪ Par ailleurs, dans le cadre du projet de partenariat transatlantique pour le commerce et l'investissement entre l'Union européenne et les Etats-Unis, le Parlement européen a adopté le 12 mars 2014 une résolution affirmant que son approbation de cet accord de libre-échange serait liée à l'arrêt par la NSA de ses activités de surveillance massive des citoyens européens (2).
▪ Le G29, groupe de travail réunissant les autorités européennes de protection des données, a rendu un avis le 10 avril 2014 relatif à la surveillance des communications électroniques, dans lequel il souligne l'illégalité de la surveillance massive, systématique et sans distinction des citoyens européens, qui ne saurait être justifiée par la seule lutte contre le terrorisme ou d'autres considérations de sécurité publique (3).

La directive conservation des données de connexion invalidée par la Cour de justice européenne

▪ La Cour de Justice de l'Union Européenne (CJUE) a rendu un arrêt, le 8 avril dernier, dans lequel elle déclare la directive 2006/24/CE relative à la conservation des données de connexion contraire aux articles 7 et 8 de la Charte des droits fondamentaux de l'Union européenne.
▪ Cet arrêt repose sur le constat que la directive, en autorisant la surveillance d'ensemble des données de communications par les Etats, ne limite pas l'impact sur les droits fondamentaux à ce qui est strictement nécessaire.
▪ La Cour ne conteste pas que la conservation des données, aux fins de permettre aux autorités compétentes de disposer d'un accès éventuel à celles-ci, répond à un objectif d'intérêt général. Cependant, elle rappelle qu'une telle ingérence n'est possible qu'à la condition que les mesures prévues soient déterminées de manière proportionnée. Or, elle juge que le texte ne remplit pas les conditions posées par ce « test de proportionnalité » (4).

Les perspectives

Au niveau national, les dispositions du droit français en matière de conservation des données de connexion demeurent applicables. Cependant, il appartient aujourd'hui à l'ensemble des autorités compétentes d'apprécier de manière circonstanciée l'impact de cette décision européenne sur le droit français.

(1) Projet de règlement européen, art. 43a

(2) Résolution du Parlement européen du 12-3-2014

(3) G29, Avis du 4/2014

(4) CJUE arrêt du 8-4-2014, affaires jointes C-293/12 et C-594/12

L'enjeu

Garantir plus de contrôle et de transparence dans les activités de surveillance des services de renseignement.

CHLOE TORRES
ALEXANDRA COTI

© ALAIN BENSOUSSAN – 2014

CONDAMNATION D'ANNUAIRES EN LIGNE POUR COLLECTE DELOYALE DE DONNEES

Des pratiques dénoncées par des plaintes auprès de la Cnil

▪ La Cour d'appel de Bordeaux vient de rappeler que la collecte déloyale de données peut donner lieu à des **sanctions pénales** (1).
▪ La Cnil précise le contexte et les détails de cette affaire dans plusieurs communiqués publiés sur son site internet, rappelant que ce dossier avait été initié par des plaintes auprès de la Cnil de nombreuses personnes (parmi lesquelles des personnes dont les coordonnées étaient sur « liste rouge »), qui avaient vu leurs noms, prénoms et coordonnées publiés dans des annuaires en ligne. La Cnil précise d'ailleurs, à cet égard, que ces plaintes avaient permis de mettre en lumière une collecte déloyale de données, les personnes concernées n'ayant jamais communiqué leurs coordonnées postales ou téléphoniques aux responsables de ces sites et n'ayant donc a fortiori pas autorisé leur mise en ligne.
▪ Après avoir effectué maintes démarches auprès des sites pour obtenir des précisions sur l'origine des coordonnées diffusées, mais également en vue de faire cesser cette collecte de données et cette diffusion, en vain, la Cnil avait saisi le procureur de la république de ces faits.
▪ Suite à cette saisine du Ministère public, l'OCLCTIC (Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication) avait été chargé d'effectuer les vérifications nécessaires à l'enquête, ce qui avait permis d'identifier et de localiser le responsable des sites internet en cause.

Une condamnation pénale assortie d'une injonction de publication

▪ En pratique, il est en effet apparu, dans le cadre de l'enquête, que les différents annuaires étaient édités par un même responsable, qui avait développé un logiciel lui permettant de collecter les données à partir de diverses sources (le journal des associations, Google, l'annuaire universel, l'INSEE), de les mettre en forme et de les diffuser dans ses annuaires en ligne.
▪ Le Tribunal correctionnel de Bordeaux avait considéré que cette pratique, consistant à recueillir les coordonnées des personnes sur les espaces publics d'internet à leur insu, constituait une collecte déloyale de données, dans la mesure où ce procédé faisait obstacle au **droit d'opposition** de ces personnes. Le défendeur avait alors interjeté appel de cette décision.
▪ La Cour d'appel de Bordeaux a confirmé le jugement de 1ère instance en condamnant le responsable des sites en cause à une peine d'amende délictuelle de 10.000 euros avec sursis, retenant plusieurs motifs et notamment des faits constitutifs de collecte de données à caractère personnel par des moyens frauduleux, déloyaux ou illicites, de traitement de données à caractère personnel malgré l'opposition légitime de la personne concernée ou encore d'abus de confiance.
▪ La Cour ordonne, en outre, la **suppression des données personnelles** des victimes déloyalement collectées et la publication de son arrêt, par extraits, par voie de diffusion internet sur le site de la Cnil, publication réalisée par la Cnil via un communiqué en date du 7 avril dernier.

Les enjeux

Outre les sanctions administratives et pécuniaires pouvant être prononcées par la Cnil en cas de traitement de données personnelles non conforme aux dispositions applicables en matière de protection des données, cette décision rappelle que des sanctions pénales sont également encourues en cas de non-respect de la loi Informatique et libertés.

(1) CA Bordeaux, 18-12-2013

Les conseils

Il est recommandé aux responsables de traitement d'effectuer régulièrement des audits de leurs pratiques en matière de collecte de données afin de s'assurer de la conformité des procédés utilisés aux dispositions applicables en matière de protection des données à caractère personnel.

LAURE LANDES-GRONOWSKI

Sources

- **La présidente de la Cnil élue présidente du G29**

La présidente de la Cnil, Isabelle Falque-Pierrotin a été élue le 27 février 2014 pour deux ns à la présidence du G29, qui réunit les représentants des autorités de protection des onnées européennes.

Isabelle Falque-Pierrotin jouera ainsi un rôle clé dans le développement de la coopération ntre les autorités de protection des données sur le plan international (1).

(1) Cnil, rubrique Actualités, art. du 27-02-2014

- **Clôture de la mise en demeure du centre commercial E.Leclerc**

Une mise en demeure avait été adoptée à l'encontre du centre commercial E. Leclerc de Bourg-en-Bresse le 12 juillet 2013 en raison du caractère disproportionné du dispositif de idéosurveillance des salariés.

Le centre commercial ayant apporté des correctifs au dispositif, la Cnil a décidé de lôturer la décision de mise en demeure (2).

(2) Cnil, rubrique Actualités, art. du 11-04-2014

- **Alerte professionnelle**

La Cnil a adopté une délibération modifiant l'autorisation unique 004 relative aux raitements automatisés de données à caractère personnel mis en œuvre dans le cadre de ispositifs d'alerte professionnelle.

Le champ d'application des dispositifs d'alerte professionnelle ne concernant auparavant ue les domaines financier, comptable, bancaire et relatif à la lutte contre la corruption, a té étendu aux pratiques anticoncurrentielles ; à la lutte contre les discriminations et le arcèlement au travail ; à la santé, hygiène et sécurité au travail ; et à la protection de environnement (3).

(3) Cnil, délibération n° 2014-042 du 30 janvier 2014 modifiant l'autorisation unique n° 2005-305 du 8 décembre 2005 n° AU-004 relative aux traitements automatisés de données à caractère personnel mis en œuvre dans le cadre de dispositifs d'alerte professionnelle

- **Réforme du règlement européen de la protection des données à caractère personnel**

. Le Parlement européen a adopté le 12 mars dernier le rapport de M. Albrecht sur le rojet de règlement relatif à la protection des données à caractère personnel ainsi que le apport de M. Droutsas sur le projet de directive. Cela démontre l'attachement du 'arlement à une réforme globale du cadre juridique de la protection des données (4).

Dans la perspective des élections européennes en mai 2014, cette adoption permet de onsolider le travail réalisé jusqu'à présent et de le transmettre au prochain Parlement. Ainsi, les députés élus en mai pourront poursuivre les travaux réalisés pendant la égislature actuelle.

Par ailleurs, le Contrôleur européen de la protection des données a publié son rapport de 'année 2013dans lequel la révision du cadre juridique des données à caractère personnel a onstitué une des priorités de 2013 et le restera en 2014.

(4) Cnil, rubrique Actualités, art. du 14-03-2014

La JTIL est éditée par Alain Bensoussan Selas, société d'exercice libéral par actions simplifiée, 58 boulevard Gouvion-Saint-Cyr, 75017 Paris, président : Alain Bensoussan.

Directeur de la publication : Alain Bensoussan – Responsable de la rédaction : Isabelle Pottier.

Diffusée uniquement par voie électronique – gratuit – ©Alain Bensoussan 2014

ISSN 1634-0698

Abonnement à partir du site : http://www.alain-bensoussan.com/outils/abonnement-petit-dejeuner-juristendance

POINT SUR LES TECHNIQUES D'ANONYMISATION

Qu'est-ce qu'un processus d'anonymisation ?

▪ On distingue les concepts d'anonymisation irréversible et d'anonymisation réversible, cette dernière étant parfois dénommée pseudonymisation.
▪ L'anonymisation irréversible consiste à supprimer tout caractère identifiant à un ensemble de données. Concrètement, cela signifie que toutes les informations directement et indirectement identifiantes sont supprimées et cela rend ainsi impossible toute ré-identification des personnes.
▪ L'anonymisation réversible est une technique qui consiste à remplacer une donnée par un pseudonyme. Cette technique permet la levée de l'anonymat ou l'étude de corrélations en cas de besoin (1).
▪ En tout état de cause, un processus d'anonymisation constitue un traitement au sens de la loi Informatique et libertés dans la mesure où des données à caractère personnel ont été initialement collectées (2).

Comment évaluer une solution d'anonymisation ?

▪ Le Groupe de l'article 29, qui regroupe des autorités de protection des données européennes, dans son avis rendu le 10 avril dernier a dégagé trois critères permettant d'évaluer une bonne solution d'anonymisation :

- L'individualisation : évaluer s'il est toujours possible d'isoler un individu ;
- La corrélation : évaluer s'il est possible de relier des ensembles de données distincts concernant un même individu ;
- La déduction : évaluer si l'on peut déduire une information sur un individu par rapport à d'autres informations.

▪ Si ces trois critères sont cumulativement remplis, le G29 considère que l'ensemble de données est bien anonyme.

▪ Si au moins un des critères n'est pas rempli, une analyse détaillée des risques de ré-identification sera nécessaire pour juger de l'efficacité de la technique d'anonymisation.

▪ Les techniques d'anonymisation sont complémentaires, il convient d'analyser au cas par cas si la combinaison des techniques utilisées présente un risque de ré-identification de la personne.

Références

(1) Cnil, guide sur la sécurité des données, fiche 16 relative à l'anonymisation

(2) G29, Avis 05/2014 du 10 avril 2014 sur les techniques d'anonymisation

Prochains événements

Dialogue compétitif : le bon outil pour les systèmes d'information du logement social : 5 juin 2014

- François Jouanneau coanime avec Jean-Baptiste Gauthier, Directeur des Systèmes d'Information de l'Estuaire de la Seine (Groupe Logeo) un petit-déjeuner débat consacré à la procédure de dialogue compétitif.
- Choisir une procédure de passation adaptée aux projets complexes constitue le premier enjeu.
- Par exemple, comment la procédure de dialogue compétitif est-elle susceptible de permettre le choix efficient d'un nouveau progiciel immobilier intégré en vue de remplacer le SI ?
- La réussite d'une procédure de dialogue compétitif passe nécessairement par la constitution d'une équipe pluridisciplinaire soudée regroupant des compétences techniques, économiques et juridiques.
- Ce petit-déjeuner débat est l'occasion d'aborder les questions suivantes :

- Comment bâtir la sécurité juridique du futur contrat par l'ajout au programme fonctionnel, de prérequis juridiques permettant aux candidats de s'exprimer sur les solutions juridiques proposées ?

- Quel est le ressenti de la maîtrise d'ouvrage publique sur la mise en œuvre, au cours de la procédure de dialogue compétitif, d'une audition spécialement dédiée aux problématiques juridiques ?

- Comment cette audition est-elle vécue par les candidats ?

- Comment ces prérequis et cette audition juridiques trouvent au final, leur traduction sur le plan contractuel ?

- Quelles sont les incidences en matière de prévention d'un futur contentieux ?

- L'objet de ce petit-déjeuner débat est donc de permettre de tirer le meilleur parti de la procédure de dialogue compétitif.
- Inscription gratuite sous réserve de confirmation avant le 3 juin 2014 à l'aide du formulaire en ligne.

Consommation : impact de la nouvelle loi sur la vente à distance : 14 mai 2014

- Céline Avignon anime un petit-déjeuner débat dédié à la nouvelle loi relative à la consommation du 17 mars 2014, dite « loi Hamon » et à son impact sur la vente à distance.
- Le commerce à distance, qu'il soit e ou m-commerce, a le vent en poupe, avec une augmentation de 75 % des transactions faites par le biais d'un mobile entre 2012 et 2013. Par ailleurs, les pouvoirs de la DGCCRF sont accrus.
- L'identification des impacts organisationnels de la réforme sur le process de commercialisation est, dans ce contexte, primordial, tant ceux-ci influencent l'activité et peuvent faire l'objet de lourdes sanctions.
- Ce petit-déjeuner est l'occasion d'identifier les principales modifications issues de la loi et leur impact sur vos process et d'examiner les questions suivantes :

- Quels sont les changements à prévoir dans vos conditions générales de vente ?

- Quelles sont les informations précontractuelles à fournir au consommateur?

- Comment formaliser le consentement du consommateur à contracter ?

- Quel délai retenir pour la livraison, le remboursement, le droit de rétractation ?

Inscription gratuite sous réserve de confirmation avant le 12 mai 2014 à l'aide du formulaire en ligne.

Formations intra-entreprise : 1e semestre 2014

Le cabinet a la qualité d'organisme de formation professionnelle depuis 30 ans[1].

Il a en outre obtenu le label Cnil « Lexing® formation informatique et libertés » pour son catalogue de formations informatique et libertés.

Informatique et libertés

- **Cil (niveau 1)** : Permettre au Cil de maîtriser les obligations et responsabilités qui lui incombent et de savoir les mettre en œuvre. — 29-05-2014
- **Informatique et libertés collectivités territoriales** : Informer les collectivités territoriales sur les modalités d'application de la réglementation Informatique et libertés. — 26-06-2014
- **Devenir Cil** : Mettre en œuvre une politique de protection des données efficace (accountability, etc.) et résoudre les questions complexes (réseaux sociaux, etc.). — 05-06-2014
- **Cil (niveau 2 expert)** : Perfectionnement et résolution de questions complexes ; acquisition de méthodologie pour exercer l'activité selon l'approche Privacy by Design. — 11-06-2014
- **Formation intra entreprise Informatique et libertés à l'attention du comité exécutif** : Sensibiliser les membres du comité exécutif aux risques Informatique et libertés liés à leur activité. — Selon demande

[1] Catalogue de nos formations 2014 sur : http://www.alain-bensoussan.com/formations-intra-entreprise/