Alain Bensoussan Avocats
Le droit du numérique et des technologies avancées

JURISTENDANCES INFORMATIQUE ET LIBERTES

n° 62 – Mars – Avril 2015

RAPPORT DE LA CNIL 2014 : BILAN ET TENDANCES

Bilan des actions et contrôles Cnil en 2014

Les enjeux

Contrôler le respect de la loi Informatique et libertés par les différents acteurs

▪ La Cnil vient de publier son 35e rapport d'activité 2014 (1). L'année 2014 a été marquée par une préoccupation croissante des Français quant à leurs données personnelles.

▪ Ainsi, la Cnil a reçu **5246 demandes de droit d'accès indirect**, soit une augmentation de 22% par rapport à 2013. Ces demandes concernent principalement le fichier FICOBA de l'administration fiscale, les fichiers d'antécédents judiciaires de la police et de la gendarmerie (fichier unique TAJ depuis le 1er janvier 2014) et les fichiers de renseignement. De plus, le nombre de plaintes est toujours aussi important puisque **5825 plaintes** ont été enregistrées, dont 39% concernent l'e-reputation.

▪ Un **nouveau service de plaintes en ligne** a été mis en place en avril 2015. Il permet de répondre aux difficultés liées à la suppression de données personnelles sur des sites, blogs, forums, réseaux sociaux ou des moteurs de recherches, ou encore aux questions relatives au spam et à la prospection commerciale par courrier, courriel ou par téléphone, aux questions de surveillance des salariés et aux inscriptions dans les fichiers d'incidents de paiement.

▪ L'année 2014 se caractérise également par les **premiers contrôles en ligne** de la Cnil. Ainsi, **58 contrôles en ligne** ont été effectués entre octobre et décembre 2014 portant notamment sur la conformité à la recommandation cookies et autres traceurs adoptée par la Cnil le 5 décembre 2013.

▪ La Cnil a également rendu un avis sur le **projet de loi relatif au renseignement**. Plusieurs recommandations de la Cnil ont été prises en compte, mais la Cnil reste attentive à l'occasion des discussions à venir sur les modifications proposées par les parlementaires, notamment celles relatives aux modalités de contrôles des fichiers de renseignements.

(1) Cnil, 35ème rapport d'activité pour 2014

Les thématiques prioritaires pour 2015

Les conseils

Réaliser un audit de conformité du dispositif aux exigences du référentiel avant de déposer un dossier de candidature.

▪ L'année 2015 s'annonce également riche en actions pour la Cnil qui entend encore augmenter le nombre de ses contrôles sur les thèmes qu'elle juge prioritaires :

- le fichier judiciaire national automatisé des auteurs d'infractions sexuelles ou violences (FIJAISV). Environ 15 missions sont planifiées pour 2015 ;
- le fonctionnement du Fichier des Incidents de remboursement de Crédits aux Particuliers (FICP). Une vingtaine de contrôles, tant sur pièces que sur place, est envisagée ;
- les traitements mis en œuvre au titre du paiement et recouvrement de l'impôt sur le revenu. La Cnil va poursuivre les missions auprès notamment d'établissements de service informatique (ESI) et de centres de données.

CHLOE TORRES

NOUVELLE AUTORISATION UNIQUE DE LA CNIL RELATIVE AUX INTERDICTIONS DE STADE

Le champ d'application de l'autorisation unique

▪ La Cnil a rendu le 7 avril dernier la délibération n°2015-118 portant autorisation unique de traitements de données à caractère personnel mis en œuvre par les associations, sociétés et fédérations sportives aux fins de gestion des interdictions de stade prononcées par l'autorité judiciaire administrative (1).

▪ L'autorisation unique AU-42 autorise les organismes mentionnés aux articles L.332-15 et L.332-16 du Code du sport à mettre en œuvre des traitements aux fins de priver les personnes frappées d'une interdiction de stade, prononcée par une juridiction ou un préfet, de la possibilité d'accéder à une enceinte dans laquelle se déroule une manifestation sportive à laquelle il leur est interdit d'assister.

▪ Les **finalités du traitement** sont « *la constitution de listes de personnes physiques faisant l'objet d'une interdiction de stade en vigueur, prononcée par une juridiction ou un préfet, et ce, afin de ne pas leur fournir un titre d'accès ou de pouvoir leur refuser l'accès à une enceinte dans laquelle une manifestation sportive est organisée* ».

▪ Les **données collectées** pourront uniquement concerner l'identification des personnes (nom, prénom, adresse, date et lieu de naissance, photographie) et des condamnations ou mesures de sûreté, à savoir :

- en cas d'interdiction judiciaire de stade : date de la décision et durée de la peine complémentaire ;
- en cas d'interdiction administrative de stade : enceintes et abords interdits d'accès, type de manifestations sportives concernées, date et durée de validité de l'arrêté préfectoral d'interdiction, le cas échéant obligation de répondre aux convocations des autorités ou des personnes qualifiées désignées par l'autorité préfectorale.

▪ Les **destinataires des données** ne pourront être que les employés du responsable de traitement qui présentent un intérêt légitime au regard de leurs attributions, en particulier les membres habilités d'un service sécurité, d'un service billetterie, d'un service juridique ou encore d'un service chargé d'organiser les rencontres et filtrer les accès d'une enceinte sportive.

Les obligations des associations, sociétés et fédérations sportives

▪ Le responsable de traitement doit **informer préalablement les personnes concernées** de son identité, la finalité du traitement, les destinataires des données et les modalités d'exercice des droits des personnes. Cette information pourra se faire par affichage, envoi ou remise d'un document, une mention dans les conditions générales de vente, une mention sur les billets ou tout autre moyen jugé plus adapté.

▪ S'agissant de la **durée de conservation** des données collectées, ces dernières ne pourront être conservées au-delà de la durée d'une interdiction de stade prononcée par l'autorité judiciaire ou administrative.

Les enjeux

L'autorisation unique AU-42 permet d'encadrer les traitements de données à caractère personnel relatif aux interdictions de stade, notamment le traitement des condamnations et mesures de sûreté.

(1) Cnil Délib. 2015-118 du 07-04-2015.

Les conseils

Vérifier que le traitement est conforme aux exigences de l'AU-42 avant de conclure un engagement de conformité sinon recourir à une demande d'autorisation normale.

CHLOE TORRES

Prochain petit-déjeuner

Sécurité et Objets Connectés : 20 mai 2015

▪ Polyanna Bigle et Nacira Salvan, responsable du pôle architecture sécurité de SAFRAN Aerospace Defense Security, animeront un petit-déjeuner sur le management de la sécurité des objets connectés. Avec une prévision de 20 milliards d'objet connectés, l'enjeu des objets connectés est aujourd'hui de créer des outils pour établir une véritable interconnexion ou un dialogue entre ces objets et ainsi dépasser le stade de la simple collection ou accumulation d'objets connectés à internet.

▪ Dans ce cadre, la sécurité va être cruciale pour agréger et analyser l'ensemble des informations produites par les objets connectés. L'utilisateur qui à terme, aura des dizaines d'objets connectés voudra, à partir d'un seul outil, administrer et consulter les données de ses différents objets.

▪ Partant du constat qu'internet n'est pas un lieu « sûr », la sécurité est au cœur de sa mise en place de tout projet. Elle prendra une importance grandissante : attaques ciblées par méls envoyés par des objets connectés, peut-être le vôtre ? hacking d'un système de climatisation à l'origine d'une énorme attaque d'une chaine de supermarchés, etc.

▪ En termes de régulation spécifique, tout est à construire ; en termes de droits liés à la sécurité, les questions se bousculent :

- Qu'en est-il de la sécurisation :
  - de l'identité des objets connectés ?
  - des données du monde physique récupérées, stockées et transférées ?
  - des transmissions d'ordre d'action, nécessitant des garanties techniques et contractuelles ?
- Quels sont les moyens de lutte contre une cybercriminalité des objets connectés ?
- Qui est responsable de quoi ?
- Qu'apporte le système de contrôle et d'acquisition de données SCADA (Supervisory Control And Data Acquisition) ?
- Comment lutter contre les failles ?

Ce petit-déjeuner sera l'occasion de faire le point sur ces questions.

▪ **Lieu :** de 9h30 à 11h00 (accueil à partir de 9h00) dans nos locaux, 58 bd Gouvion-Saint-Cyr, 75017 Paris.
▪ **Inscription gratuite** (sous réserve des places disponibles).
▪ L'enregistrement en ligne est obligatoire pour y assister : lien
▪ Vous pourrez également le voir sur notre chaîne YouTube : Lexing Alain Bensoussan Avocats : lien

NOTRE RESEAU DE CORRESPONDANTS ORGANIQUES LEXING VOUS INFORME

L'utilisation des Cookies en Italie

Lexing Italie

Studio Legale Zallone

▪ Le 8 mai 2014, l'autorité italienne de protection des données (1), le *Garante*, a publié un règlement présentant des « modalités simplifiées pour la fourniture d'informations et l'obtention du consentement en matière de cookies » (2). Ce règlement prendra effet à compter du 2 juin 2015.

▪ La réglementation italienne opère une distinction entre :

- Les **cookies techniques** qui sont utilisés exclusivement pour effectuer « la transmission d'une communication par la voie d'un réseau de communications électroniques, ou dans la mesure où cela est strictement nécessaire au fournisseur pour la fourniture d'un service de la société de l'information expressément demandé par la partie contractante ou l'utilisateur ». Ils comprennent eux-mêmes plusieurs catégories de cookies : les cookies de navigation ou de session nécessaires pour surfer sur un site donné, les cookies fonctionnels qui permettent l'activation de certains paramètres (par ex., la langue du site), ou encore les cookies analytiques qui recueillent des informations globales sur le nombre de visiteurs et la raison de leurs visites sur un site Web. Les cookies techniques ne nécessitent pas le consentement préalable des internautes.

- Les **cookies de profilage** qui sont utilisés « pour envoyer des messages publicitaires personnalisés correspondant aux préférences indiquées par l'utilisateur lors de sa navigation ». Ce type de cookie est considéré comme « très intrusif ». Par conséquent, ces cookies requièrent le recueil du consentement préalable des internautes.

▪ Les internautes doivent être informés de l'existence de cookies de profilage par une mention d'information succincte (sous forme de bandeau), puis par une notice d'information plus complète.

(1) Garante per la protezione dei dati personali: http://www.garanteprivacy.it/
(2) Règlement sur les cookies « Individuazione delle modalità semplificate per l'informativa e l'acquisizione del consenso per l'uso dei cookie », disponible en italien et en anglais sur le site Web du Garante.

L'utilisation des Cookies en Afrique du Sud

Lexing Afrique du Sud

Michalsons

▪ La loi sud-africaine sur la protection des données personnelles, la « POPI » (1) a été adoptée en 2013. Même si elle ne vise pas explicitement les cookies, ils tombent néanmoins dans son champ d'application dans la mesure où un cookie est susceptible de contenir des informations personnelles.

▪ Dans l'ensemble, la POPI repose sur le principe d'« opt-out », c'est-à-dire que le consentement des internautes avant d'installer des cookies sur leurs ordinateurs n'est pas recueilli. Il est cependant fort probable que l'Afrique du Sud se mette au diapason de la directive européenne « vie privée » en imposant le principe d' « opt-in » aux propriétaires de site Web.

▪ La POPI n'est toutefois pas encore entrée en vigueur. Une fois ce texte effectif, le Régulateur de l'information pourra émettre des règlements en vue d'encadrer l'utilisation de cookies (2). Le Régulateur de l'information (« Information Regulator ») est une nouvelle autorité de contrôle instituée par la POPI. Il dispose de pouvoirs étendus d'enquête. Les personnes concernées pourront déposer plainte auprès de cette autorité, qui sera habilitée à prendre des mesures en leur nom. Il s'agit de l'équivalent sud-africain de la Cnil française.

▪ Il semble que la POPI n'entre pas en vigueur avant mi-2015, ce qui accorderait aux entreprises jusqu'à mi-2016 pour s'y conformer (3). Toutefois, il leur est vivement recommandé de commencer d'ores et déjà le processus de mise en conformité.

(1) Protection of Personal Information Act ("POPI"). Cf. par ex. http://www.michalsons.co.za/popi-act-protection-of-personal-information/11105
(2) http://www.michalsons.co.za/information-regulator-in-south-africa/13893
(3) http://www.michalsons.co.za/popi-commencement-date-popi-effective-date/

BCR : la Cnil va délivrer des autorisations uniques aux multinationales

▪ Afin de faciliter les démarches pour les groupes multinationaux lors de transferts de données hors Union européenne, la Cnil va délivrer des autorisations uniques (1). Elles s'adresseront aux groupes ayant adopté des Règles Contraignantes d'Entreprises, ou Binding Corporate Rules (BCR).

▪ Les entités du groupe ne seront plus tenues de demander une autorisation à la Cnil pour chaque type de transfert en dehors de l'Union européenne, dès lors que les transferts de données encadrés par des BCR sont conformes à l'autorisation unique délivrée au groupe ; un simple engagement de conformité suffit.

(1) Communiqué Cnil 24-03-2015

La numérisation du commerce de détail

▪ La numérisation croissante de la consommation en magasin engendre le traitement d'un nombre grandissant de données (2), notamment dans le but de personnaliser la relation client. Cette « hyperpersonnalisation » mobilise ainsi un ensemble d'informations permettant de suivre les déplacements du client dans le magasin, connaître ses préférences, analyser son historique de transaction, simplifier la phase de paiement, etc. La Cnil souligne que ces innovations doivent s'accompagner d'une évolution dans les modalités d'exercice des droits des personnes (pastilles d'alerte lors de la géolocalisation avec possibilité de désactivation, garanties apportées lors du croisement de fichiers, etc.).

(2) Lettre Innovation et Prospective n°9, Avril 2015.

Vidéosurveillance au travail : clôture de la mise en demeure APPLE RETAIL France

▪ La Présidente de la Cnil avait adopté le 14 octobre 2014 une mise en demeure publique à l'encontre de la société Apple Retail France. Cette dernière s'est mise en conformité (masquage ou repositionnement des caméras installées dans les zones réservées aux salariés et information complète des salariés sur les dispositifs de vidéosurveillance). La mise en demeure a donc été clôturée (3).

(3) Communiqué Cnil 25-03-2015

Analyse de flux https : bonnes pratiques et questions

▪ La Cnil fait le point sur les flux https qui permettent de chiffrer des canaux de communication et donc de réduire les risques liés à l'interception de communications (4). Certains employeurs souhaiteraient pouvoir déchiffrer les flux https pour les analyser, ce que la Cnil reconnaît comme légitime. Elle précise toutefois que cette pratique doit être encadrée (information précise des salariés, gestion stricte des droits d'accès, etc.).

(4) Communiqué Cnil 31-03-2015

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

Formations intra-entreprise : 1e semestre 2015

LE CABINET A LA QUALITE D'ORGANISME DE FORMATION PROFESSIONNELLE DEPUIS 30 ANS.

Informatique et libertés	Dates
Informatique et libertés (niveau 1) : Identifier et qualifier les intervenants et les responsabilités, prévenir les risques et cerner les formalités obligatoires.	24-07 et 13-11-2015
Cil (niveau 1) : Permettre au Cil de maîtriser les obligations et responsabilités qui lui incombent et de savoir les mettre en œuvre.	14-01 et 02-04-2015
Informatique et libertés secteur bancaire : Sensibiliser les opérationnels sur les risques Informatique et libertés liés aux traitements du secteur bancaire.	20-01 et 04-03-2015
Informatique et libertés collectivités territoriales : Informer les collectivités territoriales sur les modalités d'application de la réglementation Informatique et libertés.	15-04 et 24-06-2015
Sécurité informatique et libertés : Connaître les exigences issues de la réglementation Informatique et libertés en matière de sécurité des données personnelles et sensibiliser aux risques liés à une faille de sécurité.	20-01 et 26-03-2015
Devenir Cil : Mettre en œuvre une politique de protection des données efficace (accountability, etc.) et résoudre les questions complexes (réseaux sociaux, etc.).	06-03 et 03-06-2015
Cil (niveau 2 expert) : Perfectionnement et résolution de questions complexes ; acquisition de méthodologie pour exercer l'activité selon l'approche Privacy by Design.	05-02 et 17-06-2015
Informatique et libertés gestion des ressources humaines : Donner aux membres de la direction des ressources humaines les clés pour utiliser les outils et les traitements de données personnelles mis en œuvre en matière de gestion des ressources humaines.	15-01 et 18-03-2015
Flux transfrontières de données : Présenter les dispositions qui régissent ces flux et élaborer une stratégie de gestion des flux conformément à la loi.	11-02 et 19-03-2015
Contrôles de la Cnil : Connaître l'étendue des pouvoirs de la Cnil et ses moyens de contrôle, apprendre à dialoguer avec la Cnil (notamment par le biais d'un jeu de rôle).	13-02 et 10-04-2015
Informatique et libertés secteur santé : Sensibiliser aux risques Informatique et libertés liés aux traitements du secteur santé et assurances et apporter des éléments de benchmark permettant de positionner son niveau de conformité.	27-01 et 25-03-2015
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