LEXING ALAIN BENSOUSSAN
Juristendances Informatique et Libertés
n° 55-Janv.-Fév. 2014

SANCTION DE 150 000 EUROS DE LA CNIL A L'ENCONTRE DE GOOGLE INC.

La saga Google Inc relative à la fusion de toutes ses règles de confidentialité

▪ La **formation restreinte** de la Cnil a prononcé jusqu'à présent, la plus haute sanction pécuniaire s'élevant à **150 000 euros** (1).

▪ Google Inc. a décidé le 1er mars 2013 de fusionner toutes les différentes règles de confidentialité applicables à tous ses services. A la suite d'une analyse effectuée par le G29 (groupe des Cnil européennes) concluant que la politique de confidentialité n'était pas conforme au cadre européen, le G29 a émis plusieurs recommandations le 16 octobre 2012 pour que Google se mette en conformité avec la directive européenne 95/46 (2). Ces **recommandations sont restées sans réponse**.

▪ Lors de la séance plénière du G29 du 26 février 2013, il a été décidé d'instaurer un sous-groupe de travail composé de six autorités européennes, piloté par la Cnil, en charge de poursuivre les investigations contre Google Inc. A la suite de ces investigations, les échanges avec Google n'ont pas été estimés satisfaisants.

▪ Le 17 avril 2013, la Cnil a précisé à Google Inc au nom des six autorités, que chacune d'elle mènera ses propres investigations selon ses procédures nationales et qu'il lui appartiendra de répondre à chaque correspondance qui lui est adressée.

▪ Le 20 juin 2013, la Cnil a **mis en demeure Google Inc** de modifier ses nouvelles règles de confidentialité (3).

▪ Dans ce contexte, la formation restreinte de la Cnil a prononcé une **sanction pécuniaire** à l'encontre de Google Inc pour **plusieurs manquements** à la loi Informatique et Liberté :

- La société **n'informe pas suffisamment ses utilisateurs** des conditions et finalités du traitement de leurs données personnelles. Ils ne sont pas en mesure d'exercer leurs droits.

- Aucune **durée de conservation** n'est précisée dans la politique de confidentialité de l'entreprise.

- Enfin, elle **interconnecte** toute les données qu'elle collecte.

Le caractère exceptionnel de la condamnation assortie d'une publication

▪ La Cnil considère également que Google se livre à une « **collecte déloyale** » d'informations d'utilisateurs n'ayant pas de compte Google et ignorant que les sites sur lesquels ils naviguent transmettent des informations.

▪ La condamnation a été assortie de l'obligation de **publier sous 8 jours,** la décision sur la page d'accueil française de Google **durant 48 heures** afin de la faire connaître aux utilisateurs de ses services.

▪ Google avait déposé un **recours en référé** devant le Conseil d'Etat mais a été **débouté** le 7 février 2014 (4). Le Conseil d'Etat a considéré que la publication ordonnée par la Cnil n'était pas de nature à créer pour Google un préjudice d'image et de réputation irréparable ni à nuire « à la poursuite même de son activité ou à ses intérêts financiers et patrimoniaux ».

▪ Google a donc a été **contraint d'afficher** sur sa page d'accueil française **sa condamnation** par la Cnil à 150 000 euros pour sa politique de confidentialité des données personnelles, pour une **durée de 48 heures**, à compter du samedi 8 février.

Les enjeux

Vérifier la conformité des conditions générales d'utilisation et la politique de confidentialité des entreprises avec les dispositions de la loi Informatique et Libertés.

(1) Cnil, Délib. 2013-420 du 3-1-14.

(2) Directive 95/46/CE du 24-10-95.

(3) Cf. JTIL 51 mai-juin 2013.

(4) CE 7-2-2014, ordonnance n°374595.

Les persepectives

Le projet de règlement européen visant à réformer le cadre de la protection des données renforce les sanctions. Les amendes s'échelonneront de 250 000 € (ou 0,5 % du CA mondial de l'entreprise) à 1 million d'€ (ou 2 % du CA) Cf. Alain Bensoussan, « Protection des données : décryptage du projet de règlement UE ».

CHLOE TORRES

LES NOUVELLES AUTORISATIONS UNIQUES DE LA CNIL EN MATIERE D'ASSURANCE

Le champ d'application des autorisations uniques en matière d'assurance

Les enjeux

▪ La Cnil a répondu aux besoins du **secteur de l'assurance** en matière de traitements des données sensibles, en facilitant les formalités préalables aux traitements auprès de la Cnil.

▪ Par deux délibérations du **23 janvier 2014** (1), la Cnil autorise tous les organismes d'assurance, de capitalisation, de réassurance, d'assistance, les intermédiaires d'assurance et par l'AGIRA, à accéder aux données personnelles de leurs assurés pour répondre certains besoins d'informations en matière d'assurance de personnes et d'automobile.

▪ La norme d'Autorisation Unique n°014 concerne les traitements de données à caractère personnel relatifs à la consultation du Répertoire National d'Identification des Personnes Physiques (**RNIPP**) et à l'utilisation du Numéro d'Inscription au Répertoire (NIR ou numéro de sécurité social) mis en œuvre par les organismes précités.

▪ Les **finalités du traitement** de données à caractère personnel sont *la passation, la gestion et l'exécution des contrats d'assurance, de capitalisation, et réassurance et d'assistance nécessitant la collecte et le traitement du NIR par le responsable du traitement* notamment pour :

- Leurs activités d'assurance maladie, maternité, invalidité, retraite supplémentaire
- Leurs activités d'assurance pour les garanties perte d'exploitation et perte d'emploi uniquement à des fins probatoires
- Les relations avec les professionnels, les établissements et les institutions de santé
- Les déclarations sociales des entreprises souscriptrices de contrats d'assurance
- L'indemnisation des accidents
- La gestion des rentes
- Pour l'exécution des dispositions légales, réglementaires et administratives en vigueur.
- L'accès aux données du RNIPP
- Et les traitements mise en œuvre par l'AGIRA ayant des objets prédéfinis.

▪ L'Autorisation Unique n°15 concerne les traitements de données à caractère personnel relatifs aux infractions, condamnations ou mesures de suretés qui influencent la souscription ou la vie du contrat ou qui sont utiles pour la gestion des contentieux, mis en œuvre par les organismes précités.

Les entreprises concernées disposent d'un délai de 18 mois à compter de la publication des autorisations uniques pour se mettre en conformité, soit jusqu'au 7 août 2015.

(1) Cnil, Délib. 2014-014 et Délib. 2014-015 du 23-01-14.

Les obligations des organismes d'assurance

Les conseils

▪ Le **responsable du traitement** doit informer préalablement les personnes concernées

- de son identité,
- de la finalité du traitement,
- du caractère obligatoire ou facultatif des réponses,
- des conséquences éventuelles d'un défaut de réponse,
- des destinataires des données, de leur droit d'accès, de rectification et d'opposition et
- de l'éventuel transfert de données personnelles à destination d'un Etat non membre de l'UE.

▪ S'agissant de la **durée de conservation** des données collectées, ces dernières doivent être conservées par le responsable de traitement pour la durée nécessaire à l'exécution du contrat.

Vérifier que le traitement est conforme aux exigences des AU 014 et 015 avant de conclure un engagement de conformité sinon recourir à une demande d'autorisation normale.

CHLOE TORRES

L'entrave aux actions de la Cnil entraîne une sanction pécuniaire

Sources

▪ Le **7 janvier 2014**, la Cnil a rendu publique les sanctions pécuniaires de quatre sociétés pour un montant total de **33 000 euros** pour avoir entravé l'action de la commission et commis divers manquements.

▪ Les trois premier cas concernent des systèmes de **vidéosurveillances abusives**. Le dernier est relatif à un système de **géolocalisation** installé dans le véhicule de l'entreprise qui ne pouvait être désactivé en dehors des heures de travail (1).

▪ Ces sanctions font suite à divers rappels et mises en demeure de la Cnil sur les obligations que doivent respecter les responsables de traitement au titre de la loi « Informatique et Libertés » précédés par des **plaintes des salariés** des sociétés.

(1) Cnil, délib. 2013-319 et 2013-320 du 24-10-2013 ; délib. 2013-366 du 23-11-2013 et délib. 2013-400 du 12-12-2113

Surveillance excessive des salariés : mise en demeure de la Cnil

▪ La Cnil, après un contrôle consécutif d'une **plainte**, a mis en demeure une société exploitant un centre commercial compte tenu des manquements et du **caractère intrusif** des dispositifs installés dans un centre commercial (2).

▪ La société ne pouvait utiliser le **dispositif biométrique** pour contrôler les horaires des salariés. Les empreintes des salariés ayant quitté l'entreprise sont conservées de manière excessive.

▪ Le dispositif de vidéosurveillance est disproportionné puisque les salariés sont sous surveillance de manière permanente. Les salariés ont été insuffisamment informés du dispositif (3). Aucun de ces dispositifs n'a été déclaré à la Cnil.

(2) Cnil, Déc. 2014-001 du 15-1-14

(3) Cf : FAQ, p. 4.

Réunion des principaux opérateurs de communication électronique de Cnil

▪ La Cnil a réuni le **3 février 2014** les principaux opérateurs de communication électronique pour rappeler leurs obligations en matière de violation des données personnelles en vue de respecter les dispositions de la loi Informatique et libertés. Celle-ci impose aux fournisseurs de services de communications électroniques de notifier à la commission toute **violation de données personnelles** et le cas échéant, d'informer les personnes concernées de l'existence de la violation (4).

▪ Un règlement européen entré en vigueur en aout 2013 précise les délais, le contenu et les modalités de cette notification (5).

▪ La Cnil met à la disposition une **téléprocédure sécurisée**.

(4) Art 34 bis de la Loi n°78-17 modifiée.

(5) Règlement européen n°611/201.

Journée de la protection des données : 8ème édition

▪ Chaque année, le **28 janvier** a été célébré la journée de la protection des données instituée en 2006 par le Comité des Ministres du Conseil de l'Europe. Il s'agit de la date anniversaire de l'ouverture à la signature de la Convention 108 du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel.

▪ Pour cette occasion, le « **manuel de droit européen** en matière de protection des données à caractère personnel » est disponible sur le site du Conseil de l'Europe (6).

(6) Manuel de droit européen en matière de protection des données à caractère personnel.

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 2013

ISSN 1634-0698

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

POINT SUR VIOLATION DE DONNEES PERSONNELLES ET LA VIDEOSURVEILLANCE AU TRAVAIL

Comment les fournisseurs de communications électroniques mettent ils en œuvre leur obligation de notifier la violation de données personnelles ?

Références

▪ La violation de données à caractère personnel est définie comme *toute violation de la sécurité entraînant accidentellement ou de manière illicite la destruction, la perte, l'altération, la divulgation ou l'accès non autorisé à des données à caractère personnel faisant l'objet d'un traitement dans le cadre de la fourniture au public de services de communications électroniques* (1).

▪ Le fournisseur de communications électroniques doit :

▪ **Notifier à la Cnil** la violation de données personnelles **dans les 24 heures** de sa constatation. Une notification en deux temps est possible s'il ne dispose pas de toutes les informations requises : une notification complémentaire comprenant toutes les informations doit être faite dans les 72 heures après la notification initiale.

(1) Art 34 bis de la Loi n°78-17 modifiée.

▪ **Informer les personnes concernées** par la violation sauf si elle ne porte pas atteinte aux données ou à la vie privée des personnes ou si des mesures techniques de protection appropriées sont mise en place préalablement par le fournisseur. La Cnil peut imposer au fournisseur de le faire.

▪ **Tenir à jour un inventaire des violations** indiquant les modalités de la violation, ses effets et conséquences et les mesures prises pour remédier à la violation. Cet inventaire doit être conservé à la disposition de la Cnil.

Comment un dispositif de vidéosurveillance peut-il être mis en place au travail ?

▪ Tout système de vidéosurveillance doit respecter le **principe de proportionnalité** et doit s'effectuer de façon adéquate, pertinente, non-excessive et strictement nécessaire à l'objectif poursuivi. Généralement le déploiement de ce dispositif aura un objectif sécuritaire des biens et des personnes.

▪ La Cnil rappelle que la mise en place de ce dispositif ne peut avoir pour seul objectif la mise sous surveillance d'un employé spécifique ou un groupe particulier d'employés et prend en compte le nombre de caméras, leur emplacement, leur orientation, leurs fonctionnalités, leurs périodes de fonctionnement pour savoir s'il y a manquement à la loi « Informatique et liberté ».

▪ Le responsable de traitement doit **déclarer son traitement** à la Cnil. Il a une obligation d'informer les salariés et les visiteurs de la mise en place du système de surveillance.

(2) Cnil, Délib. n°2009-201 du 16-4-2009.

▪ L'information doit apparaître de manière visible dans les locaux sous surveillance et elle doit mentionner les destinataires des images, les modalités concrètes d'exercice de leur droit d'accès pour les images les concernant.

▪ Les instances représentatives du personnel doivent également être consultées avant toute mise en œuvre d'un système de vidéo surveillance.

▪ La Cnil préconise une durée de conservation des images de 1 mois maximum.

▪ LA Cnil a déjà condamné à **10 000 euros** une société pour ne pas lui avoir déclaré un système de vidéosurveillance qui filmait les salariés de **manière permanente** sans les avoir informé (2).

Données personnelles : les impacts du futur règlement européen : le 20 mars 2014

▪ André Meillassoux, Président de l'Association française du droit de l'informatique et de la télécommunication (AFDIT) et Alain Bensoussan organisent le 20 mars 2014 un colloque sur le thème "Données personnelles: les impacts du futur règlement européen" avec le concours d'Ubifrance.

▪ La Commission européenne a publié le 25 janvier 2012 un projet de règlement général sur la protection des données qui a vocation à réviser le cadre européen de la protection des données à caractère personnel. Le texte définitif pourrait être publié d'ici fin 2013 et adopté en mai 2014.

▪ Les points clés de la proposition sont les suivants :

- l'obligation sous certaines conditions tenant à la taille de l'entreprise ou aux traitements mis en œuvre de désigner un délégué à la protection des données ;
- la consécration d'un droit à l'oubli numérique pour les personnes concernées ainsi qu'un droit à la portabilité des données;
- l'application du principe d'accountability ;
- l'obligation de la mise en œuvre de la protection des données dès la conception et par défaut ;
- l'introduction de l'obligation de notification des violations de données à caractère personnel.

▪ Cette proposition implique pour les entreprises d'adopter certaines mesures permettant de se préparer au futur renforcement des obligations.

▪ Cette journée a pour objet de présenter les points clés de la proposition de règlement et les mesures à mettre en place pour anticiper son adoption.

▪ Alain Bensoussan et Chloé Torres interviendront aux côtés de Christian Pardieu (GE Corporate), Patricia Le Large (Orange), Hélène Legras (Areva), Emmanuelle Bartoli (Atos), Dominique Entraygues et José Patrick Boé (Michelin), Serge Yablonsky (SYC Consultants), Fabien Gandrille (SCOR SE), Jacques Perret (GDF Suez), Bertrand Lapraye (Alcatel Lucent) et Jean-François Simon (Nestlé).

▪ Edouard Geffray, secrétaire de la Cnil, clôturera cette journée.

▪ Lieu : Ubifrance,
77 boulevard Saint-Jacques
75014 Paris
▪ Programme et inscription auprès de l'AFDIT

Formations intra-entreprise : 1er 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

▪ **Informatique et libertés (niveau 1)** : Identifier et qualifier les intervenants et les responsabilités, prévenir les risques et cerner les formalités obligatoires.	09-01 et 03-04-2014
▪ **Cil (niveau 1)** : Permettre au Cil de maîtriser les obligations et responsabilités qui lui incombent et de savoir les mettre en œuvre.	13-02 et 29-05-2014
▪ **Informatique et libertés secteur bancaire** : Sensibiliser les opérationnels sur les risques Informatique et libertés liés aux traitements du secteur bancaire.	22-01 et 26-03-2014
▪ **Informatique et libertés collectivités territoriales** : Informer les collectivités territoriales sur les modalités d'application de la réglementation Informatique et libertés.	05-02 et 26-06-2014
▪ **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.	16-01 et 13-03-2014
▪ **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 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.	05-03 et 11-06-2014
▪ **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.	08-01 et 11-03-2014
▪ **Flux transfrontières de données** : Présenter les dispositions qui régissent ces flux et élaborer une stratégie de gestion des flux conformément à la loi.	17-01 et 27-03-2014
▪ **Contrôle 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).	14-02 et 04-04-2014
▪ **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.	23-01 et 21-03-2014
▪ **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/secteurs-dactivites/formation-intra-entreprise