Alain Bensoussan Avocats
Le droit du numérique et des technologies avancées

JURISTENDANCES INFORMATIQUE ET LIBERTES

n° 64 – Juillet – Août 2015

METHODOLOGIE POUR FAIRE FACE AUX OBLIGATIONS EN MATIERE DE FAILLES DE SECURITE

Le référentiel normatif et documentaire en matière de sécurité des systèmes d'information

▪ L'article 34 de la loi Informatique et libertés impose au responsable de traitement une obligation générale de sécurité qui recouvre l'intégrité et la confidentialité.
▪ Au titre de l'intégrité, le responsable de traitement doit éviter que les données soient endommagées (intégrité physique) et déformées (intégrité logique). Le respect de l'obligation de confidentialité suppose, quant à lui, une politique de gestion des droits d'accès aux données rigoureuse afin de pouvoir définir les tiers autorisés.
▪ Chaque responsable doit identifier les risques engendrés par son traitement avant de déterminer les moyens adéquats pour les réduire. Pour ce faire, il convient d'adopter une vision globale et d'étudier les conséquences sur les personnes concernées.
▪ La **norme ISO 27001** détaille les exigences relatives à l'établissement, la mise en œuvre, le fonctionnement, la surveillance et le réexamen, la mise à jour et l'amélioration d'un système de management de la sécurité de l'information (SMSI) (1).
▪ Un SMSI désigne l'approche systémique par laquelle une organisation veille à la **sécurité des informations sensibles**. Construit selon un processus de management du risque, un SMSI englobe les personnes, les processus et les systèmes de TI. Les exigences fixées dans l'ISO 27001:2013 sont génériques et prévues pour s'appliquer à toute organisation, quels que soient son type, sa taille et sa nature.
▪ Il est également possible de se référer aux normes **ISO 27002** et **ISO 31000** (2) ainsi qu'au **Référentiel de bonnes pratiques de l'Afnor** intitulé « Prévention et gestion de la fuite d'informations - Protection du patrimoine informationnel » (3).

Les recommandations de la Cnil

▪ Le management du risque est une préoccupation importante de la Cnil qui impose, dans son référentiel de labellisation des audits, que la procédure d'audit comprenne :
▪ « une démarche particulière pour identifier les principaux risques que les traitements dans le champ de l'audit font peser sur les libertés et la vie privée des personnes concernées en cas d'atteinte à la sécurité des données à caractère personnel, en tenant compte des éventuels sous-traitants. Cette démarche permet notamment d'estimer ces risques en termes de gravité et de vraisemblance » (4).
▪ Son guide méthodologique sur la gestion des risques révisé en 2015 atteste également de l'importance de cette problématique pour cette dernière selon laquelle le niveau de risque doit être estimé en termes de gravité et de vraisemblance (5).
▪ Ce nouveau guide tient compte du projet de règlement européen sur la protection des données et les réflexions du G29 sur l'approche par les risques.
▪ Il tient aussi compte des retours d'expérience et des améliorations proposées par différents acteurs.
▪ La Cnil propose ainsi une méthode encore plus efficace se composant de deux guides : la **démarche méthodologique** et l'**outillage** (modèles et exemples) (6).

Les enjeux

La négligence ou l'absence de mesures de sécurité peuvent être sanctionnées de 300 000 euros d'amende et de 5 ans d'emprisonnement.

(1) Pour avoir un aperçu de la norme ISO 27001:2013.

(2) Liste des normes de système de management sur le site de l'ISO.

(3) Prévention de la fuite d'information, BP Z90-001, janvier 2015.

(4) Cnil, Délib. 2011-316 du 6-10-2011.

Les conseils

La démarche d'analyse des risques doit être effectuée préalablement afin de pouvoir déterminer les mesures de sécurité à mettre en œuvre.

(5) Cnil, Guide « Gérer les risques sur les libertés et la vie privée », éd. 2015.
(6) Documents disponibles sur le site de la Cnil.

EMMANUEL WALLE

DECLARATION A LA CNIL ET GEOLOCALISATION DES SALARIES

Principales conditions de la nouvelle délibération Cnil

▪ **Finalités du traitement**. La géolocalisation ne peut être mise en œuvre que pour tout ou partie des finalités suivantes :

- le respect d'une obligation légale ou réglementaire imposant la mise en œuvre d'un dispositif de géolocalisation en raison du type de transport ou de la nature des biens transportés ;
- le suivi et la facturation d'une prestation de transport de personnes ou de marchandises ou d'une prestation de services directement liée à l'utilisation du véhicule, ainsi que la justification d'une prestation auprès d'un client ou d'un donneur d'ordre ;
- la sûreté ou la sécurité du salarié lui-même ou des marchandises ou véhicules dont il a la charge, en particulier la lutte contre le vol du véhicule ;
- une meilleure allocation des moyens pour des prestations à accomplir en des lieux dispersés, notamment pour des interventions d'urgence ;
- le contrôle du respect des règles d'utilisation du véhicule définies par l'employeur ;
- à titre accessoire uniquement, le suivi du temps de travail, lorsque ce suivi ne peut être réalisé par un autre moyen et que les salariés ont été dûment informés de sa finalité.

▪ **Période transitoire.** Les entreprises ayant déjà effectué une déclaration simplifiée en référence à la précédente norme ont **jusqu'au 17 juin 2016** pour se mettre en conformité avec les nouvelles conditions posées par la Cnil.

Quelles sont les données qui peuvent être collectés et traités ?

▪ **Données collectées :**

- l'identification du salarié (nom, prénom, coordonnées professionnelles, matricule interne, numéro de plaque d'immatriculation du véhicule) ;
- les données relatives à ses déplacements (données de localisation, historique des déplacements effectués) ;
- les données complémentaires associées à l'utilisation du véhicule (vitesse de circulation du véhicule, nombre de km parcourus, durées d'utilisation du véhicule, temps de conduite, nombre d'arrêts), sachant toutefois que, sauf si une disposition légale le permet, le traitement de la vitesse maximale ne peut pas s'effectuer ;
- la date et l'heure d'une activation et d'une désactivation du dispositif de géolocalisation pendant le temps de travail.

▪ **Limites.** La géolocalisation ne peut permettre de :

- de collecter des données de localisation en dehors du temps de travail du salarié, dont ceux résultant des trajets domicile - lieu de travail ou pendant ses temps de pause ;
- de suivre le temps de travail du salarié sauf si ce suivi ne peut être réalisé par un autre moyen, et que ces derniers ont été dûment informés, ainsi que les institutions représentatives du personnel.

▪ **Sécurité des données.** La CNIL pose également certaines recommandations concernant la préservation de la sécurité des données et leur durée de conservation.

Les enjeux

Face à l'évolution des pratiques en matière de géolocalisation des véhicules utilisés par les salariés, la Cnil a adopté une nouvelle délibération n°2015-165 du 4 juin 2015, venant compléter la norme du 16 mars 2006, relatives aux conditions permettant de bénéficier du régime de la déclaration simplifiée.

(1) Délib. 2015-165 du 4-6-2015, JO du 17-6-2015.

Les conseils

Auditer des dispositifs de géolocalisation.
Vérifier l'existence d'une déclaration à la Cnil, l'information des salariés et IRP.

Vérifier la conformité du dispositif déclaré à la nouvelle délibération de la Cnil.

EMMANUEL WALLE
PRISCILLA GUETTROT

LA DECLARATION SIMPLIFIEE ET LA GEOLOCALISATION

Toutes les données personnelles obtenues par le système de géolocalisation peuvent-elles être collectées ?

▪ **Non**. Pour ne pas porter atteinte au respect de l'intimité de la vie privée, il n'est pas possible de collecter une donnée de localisation en dehors du temps de travail.

▪ Notamment lors des trajets effectués entre le domicile et le lieu de travail de l'employé.

Les employés ont-ils la possibilité de désactiver le système de géolocalisation ?

▪ **Oui**. En particulier à l'issue du temps de travail ou pendant leur temps de pause. Le responsable du traitement pourra, le cas échéant, demander des explications en cas de désactivation trop fréquente ou trop longue du dispositif.

Le dispositif peut-il être utilisé pour le suivi du temps de travail ?

▪ **Oui.** Lorsque que ce ne peut être réalisé par un autre moyen, sous réserve de ne pas collecter ou traiter des données de localisation en dehors du temps de travail.

Références

(1) Délib. 2015-165 du 4-6-2015, JO du 17-6-2015.

Prochain petit-déjeuner

Informatique et libertés : Bilan d'activité de la Cnil (2e session) : 16 septembre 2015

▪ Alain Bensoussan animera un petit-déjeuner débat consacré à la présentation du bilan d'activité de la Cnil pour l'année 2014.

▪ L'année 2014 a confirmé la tendance observée depuis quelques années quant à l'augmentation des activités de contrôle et de sanction de la Cnil. Pour 2015, la Commission se fixe un objectif d'environ 550 contrôles se décomposant de la façon suivante :

- environ 350 vérifications sur place, dont un quart sur les dispositifs de vidéoprotection ;
- 200 contrôles en ligne.

▪ Parmi les thématiques prioritaires des contrôles figurent les « Binding Corporate Rules » (BCR). Ce qui permettra à la Cnil d'avoir un éclairage sur l'impact du dispositif au regard de la protection des données et du respect de la vie privée au sein des groupes concernés. De plus, les plaintes sont toujours aussi importantes (5800 en 2014).

▪ Au-delà de ces chiffres, l'année 2014 se caractérise par les initiatives de la Cnil pour accompagner les entreprises dans leur démarche de conformité à la réglementation Informatique et libertés :

- publication du label « Gouvernance Informatique et Libertés ;
- élaboration du pack de conformité assurance.

▪ L'année 2015-2016 s'annonce aussi riche en actions au vu du programme des contrôles annoncés par la Cnil.

▪ Nous vous proposons, dans le cadre de ce petit-déjeuner, de préciser les actions à mettre en œuvre pour assurer la conformité de leur activité à la réglementation Informatique et libertés et anticiper l'adoption du projet de règlement européen en matière de protection des données qui devrait être adopté fin 2015.

▪ **Lieu :** de 9h30 à 12h00 (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 : formulaire en ligne.

▪ A cette occasion, découvrez en vidéos le Code Informatique, fichiers et libertés, paru dans la collection Lexing - Technologies avancées & Droit, aux éditions Larcier.

▪ Notre éditeur nous invite à vous proposer l'offre spécifique qu'il a créée pour cet événement. Souscrivez au Code enrichi lors de l'inscription et bénéficiez d'une remise de 5 %, cliquez ici.

▪ **Open data : enjeux et risques juridiques : 23 septembre 2015**

▪ Laurence Tellier-Loniewski animera un petit-déjeuner débat sur comment profiter des opportunités et éviter les pièges juridiques et contractuels ?

▪ L'ouverture des informations publiques, sous l'impulsion de l'Union européenne, favorise l'émergence de nouveaux produits et services et a un impact économique direct et indirect considérable. Ces perspectives ne doivent cependant pas faire oublier que le régime juridique des données publiques ou accessibles au public est complexe, le terme « open data » s'avérant parfois trompeur et la multiplicité des licences open data n'en facilitant pas la compréhension.

▪ La privatisation des données par le droit de la propriété intellectuelle est également une tendance de notre droit :

- Que faut-il entendre par « open data » ?
- Les personnes publiques peuvent-elles refuser de communiquer les données qu'elles détiennent ?
- Peut-on privatiser des données ? Qui en est propriétaire ?
- Quelles sont les principales licences « open data » ?

▪ Telles sont notamment les questions qui seront abordées lors du petit-déjeuner.

▪ **Lieu :** de 9h30 à 12h00 (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 : formulaire en ligne.

NOTRE RESEAU DE CORRESPONDANTS ORGANIQUES LEXING VOUS INFORME

Cybersécurité et protection des données en Grèce

▪ **Ballas, Pelecanos & Associates LPC** contribue à la première édition de « La vie privée, la protection des données et de la cybersécurité Law Review » (Law Business Research Ltd).

▪ Le chapitre relatif à la **législation Grecque** couvre tous les aspects pertinents de la vie privée, la protection des données et de la cybersécurité avec un accent particulier sur les questions de données et de la vie privée en ligne (Télécharger le chapitre).

▪ La première édition de cet ouvrage apparaît à un moment de changement de politique extraordinaire et de défi dans le domaine de la **protection des données personnelles**.

▪ Aux États-Unis, les violations de données massives ont rivalisé avec les lanceurs d'alerte et l'affaire Edward Snowden. En Europe, le « droit à l'oubli », et les nouvelles règles draconiennes proposées dans le projet de règlement sur la protection des données, ont considérablement modifié le paysage politique. Cet ouvrage arrive à point nommé.

(1) Actualité du 01-07-2015.

Lexing Grèce
Ballas, Pelecanos & Associates LPC

Éviter les pièges du Data Mining aux Etats-Unis

▪ **Françoise Gilbert** a été interviewé par le magazine Compliance Week dans le cadre d'un dossier sur les pièges du Data Mining pour les entreprises (2).

▪ Afin de réduire leur risque de responsabilité découlant d'un litige, Françoise conseille aux entreprises de faire preuve de transparence au sujet de leurs pratiques de manipulation de données.

▪ **Ainsi, l**es consommateurs devraient être informés que des informations personnellement identifiables sont recueillies, pourquoi elles le sont et avec qui elles sont susceptibles d'être partagées.

▪ Ces derniers mois, de nombreuses entreprises se sont retrouvées la cible d'actions en justice qui auraient facilement pu être évitées. Beaucoup de ces plaintes portent sur le fait de ne pas avoir obtenu le consentement approprié des personnes pour collecter leurs données personnelles, ou encore d'avoir outrepassé les limites du consentement, en n'offrant pas aux individus le **droit d'opt-out**.

▪ Françoise Gilbert met en évidence la façon dont le concept de « **privacy by design** » (issu du projet de règlement communautaire en voie d'être adopté) devrait être appliqué par les entreprises lorsqu'elles développent un nouveau site web ou une **application mobile**.

▪ Cette approche se traduit par la prise en compte de la protection de la vie privée par des mesures de protection incorporées et intégrées **dès la conception** et le développement d'un produit et non après coup, une fois le produit lancé.

(2) Actualité du 14-7-2015.

Lexing Etats-Unis
IT Law Group

Premier bilan des contrôles sur les cookies

▪ La Présidente de la Cnil a **mis en demeure** une **vingtaine d'éditeurs** de sites internet qui ne respectent pas les règles encadrant l'utilisation des cookies et autres traceurs, à la suite des nombreux contrôles qu'elle a réalisés fin 2014 (1).
▪ Elle précise qu'une mise en demeure n'est pas une sanction et qu'aucune suite ne sera donnée à cette procédure si le site se conforme à la loi dans le délai imparti. Selon la Cnil, les premières réponses apportées par les sites internet concernés témoigneraient d'une volonté de se mettre en conformité.

(1) Communiqué Cnil du 30-6-2015.

Avis du G29 sur l'usage des drones

▪ Dans un avis du **16 juin 2015**, le Groupe des Cnil européennes (G 29) fait des recommandations sur les questions de protection de la vie privée et des données relatives à l'utilisation des drones (2).
▪ Plusieurs risques d'atteinte à la vie privée existent en ce qui concerne le traitement des données par les équipements à bord d'un drone. Après avoir précisé la portée de l'avis à la lumière des dérogations prévues par la directive 95/46/CE, le G29 fournit des lignes directrices permettant de tenir compte des règles de protection des données dans le contexte de drones.

(2) G29 WP 231 Avis 01-2015 16 06 2015 Privacy and Data Protection issues relating to the utilisation of Drones (en).

Accès au fichier des antécédents judiciaires et personnes recherchées

▪ Le décret 2015-648 du **10 juin 2015** sur l'accès au traitement d'antécédents judiciaires et au fichier des personnes recherchées (3) permet aux personnels investis de missions de police administrative individuellement désignés et spécialement habilités par le représentant de l'Etat, dont font partie les agents du CNAPS et les agents de préfecture, d'avoir désormais un accès plus large aux informations figurant dans le traitement des antécédents judiciaires.

(3) Décr. 2015-648.

Google mis en demeure par la Cnil

▪ La Cnil a mis en demeure Google le **8 juin 2015**, de procéder, dans un délai de 15 jours, au déréférencement des demandes favorablement accueillies sur l'ensemble du traitement et sur toutes les extensions du moteur de recherche (4).
▪ Elle considère en effet que l'arrêt de la CJUE du 13 mai 2014 sur le déréférencement concerne toutes les extensions. Un an après l'arrêt, Google a donné suite à de nombreuses demandes de déréférencement, mais seulement sur les « extensions » européennes du moteur de recherche.

(4) Délib. 2015-170 du 8-6-2015 sur la mise en demeure de la société GOOGLE INC.

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 : 2e semestre 2015

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

Informatique et libertés

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