LEXING ALAIN BENSOUSSAN
Juristendances Informatique et Libertés
n° 54-Nov.-Déc. 2013

LE REGLEMENT EUROPEEN SUR LA PROTECTION DES DONNEES : UNE NOUVELLE ETAPE

Les députés européens renforcent la protection des données dans l'UE

Enjeux

▪ La Commission des libertés civiles, de la justice et des affaires intérieures (LIBE) a adopté le **21 octobre 2013** sa position au sujet de la proposition de règlement européen sur la protection des données (1).

▪ Pour que les citoyens contrôlent leurs données personnelles et que les entreprises se déplacent plus facilement dans l'UE, les députés européens ont adopté en commission des libertés civiles, une **révision des règles** sur la protection des données.

Réviser la directive de 1995 en actualisant les principes juridiques sur la protection des données afin de prendre en compte les défis posés par internet.

▪ Il convient de rappeler que la réforme des règles européennes sur la protection des données (dite « paquet sur la protection des données ») s'articule autour de **deux projets** législatifs :

- un **règlement général** sur le traitement des données personnelles au sein de l'UE (secteur public et secteur privé) ;

- une **directive** sur la protection des données qui vise à prévenir, détecter ou poursuivre les infractions pénales ainsi qu'à appliquer les peines (application de la loi).

▪ Les règles actuellement en vigueur sont issues de la **directive 95/46/CE** sur la protection des données qui date du 24 octobre 1995. Ces dispositions ont été adoptées il y a 17 ans, lorsque moins de 1 % des Européens utilisaient l'internet.

(1) Fiche de procédure sur europarl

▪ Elles ne prennent donc pas en compte les nouvelles exigences de l'environnement numérique et ne couvrent pas non plus le cas des données traitées à des fins d'exécution de la loi.

Une révision des règles sur la protection des données

Objectif

▪ Les députés européens ont notamment introduit :

- des **sauvegardes** pour les **transferts** de données aux pays tiers,

- l'obligation d'avoir un **consentement explicite**,

- le **droit à l'effacement** et

- des **amendes plus élevées** pour les entreprises violant les règles.

L'objectif du Parlement européen est de conclure un accord sur cette importante réforme législative avant les élections européennes de mai 2014.

▪ Ainsi, les entreprises qui ne respectent pas les dispositions du règlement seraient passibles d'une sanction financière allant **jusqu'à 100 millions d'euros** ou 5 % du chiffre d'affaires annuel mondial.

▪ Les données à caractère personnelles d'une personne **devraient être effacées** si elle en fait la demande. Par ailleurs, si une personne concernée demande au responsable de traitement d'effacer ses données, l'entreprise devrait également envoyer la demande aux parties qui dupliquent les données.

▪ La désignation d'un **délégué à la protection des données** serait **obligatoire** pour les entreprises qui traitent des données de plus de 5 000 personnes physiques par an.

▪ Enfin, parmi les autres éléments introduits par les députés, figure le retrait de la possibilité d'établir des BCR sous-traitant.

CHLOE TORRES

NOUVELLE RECOMMANDATION DE LA CNIL RELATIVE AUX CARTES DE PAIEMENT

Le champ d'application de la nouvelle recommandation de la Commission

▪ Au regard de l'évolution du cadre légal et technologique depuis ces dix dernières années, la Cnil a récemment actualisé ses recommandations s'agissant des garanties minimales à respecter lors de la mise en œuvre, par les professionnels, de **traitements afférents à des données relatives à la carte de paiement** (1).

▪ La délibération du 14 novembre 2013, qui vise les traitements de données relatives à la carte de paiement en matière de **vente de biens ou de fourniture de services à distance**, abroge une délibération du 19 juin 2003 portant adoption d'une recommandation relative au « *stockage et à l'utilisation du numéro de carte bancaire dans le secteur de la vente à distance* ».

▪ La recommandation s'applique au traitement de données relatives à la carte de paiement (carte interbancaire ou dispositif similaire), lors de la vente d'un bien ou la fourniture d'une prestation de service conclu(e) sans la présence physique simultanée des parties, entre un consommateur (personne physique) et un professionnel qui, pour la conclusion de ce contrat, utilisent exclusivement une ou plusieurs techniques de communication à distance (internet, téléphone, etc.)

▪ Les cartes de paiement visées sont celles qui permettent notamment d'effectuer des achats chez un commerçant ou un prestataire de services affiliés à un réseau de paiement national ou international (système CB , Visa, Mastercard, etc.) mais aussi les **cartes de paiement dites privatives** (cartes émises par les commerçants ou par les établissements financiers spécialisés dans le crédit à la consommation) **et accréditives** (carte présentée par un adhérent à un fournisseur affilié au réseau de l'émetteur de la carte).

▪ Certaines finalités de traitement des informations « CB » liées à la particularité des opérations à distance sont clairement mentionnées car considérées comme légitimes par la Cnil (la réservation d'un bien ou d'un service, ou encore la facilitation des éventuels achats ultérieurs du client sur le site du commerçant).

▪ Les modalités de mise en œuvre des traitements visant à **lutter contre la fraude** grâce au numéro de la carte de paiement sont précisées.

▪ Le **numéro de la carte de paiement** ne peut pas être utilisé comme identifiant commercial et seuls le numéro de la carte, la date d'expiration et le cryptogramme visuel constituent des données nécessaires à la réalisation d'une transaction à distance par carte de paiement, à l'exclusion de l'identité du titulaire de la carte et de la photocopie ou de la copie numérique de la carte de paiement qui ne doivent pas, par principe, être collectées (2).

Les obligations des e-commerçants en matière de conservation des données

▪ S'agissant de la durée de conservation des données, la Cnil rappelle que les données relatives à la carte ne peuvent être conservées que pendant la durée nécessaire à la réalisation de la transaction.

▪ Les commerçants en ligne peuvent conserver le numéro et la date de validité de la carte, à l'exclusion du cryptogramme visuel, à des fins de gestion des éventuelles réclamations des titulaires de cartes de paiement pendant treize ou quinze mois suivant la date de débit sous forme d'**archives intermédiaires**.

▪ Lorsque les données relatives à la carte sont conservées au-delà du temps strictement nécessaire à la réalisation de la transaction, pour simplifier un paiement ultérieur, le responsable du traitement doit recueillir le **consentement libre, spécifique et informé** de la personne concernée. Il doit également intégrer directement sur son site marchand un moyen simple de retirer, sans frais, le consentement donné pour la conservation des données de la carte.

Enjeu

La sécurité et la confidentialité des données relatives aux cartes de paiement constituent des éléments clés pour garantir la confiance dans le commerce électronique.

(1) Cnil, Délib. 2013-358 du 14-11-2013.
(2) Cf. le FAQ p.4 du présent numéro.

Objectif

La délibération précise les recommandations de la Cnil et les garanties minimales à respecter lors de la mise en œuvre, par les professionnels, de traitements afférents à des données relatives à la carte de paiement.

CELINE AVIGNON
RAOUF SAADA

Cookies : publication d'une recommandation de la Cnil

▪ La Cnil a présenté, le **16 décembre 2013**, une recommandation visant à préciser les obligations des responsables de sites internet en vue de leur permettre de se mettre en conformité avec les dispositions de la loi Informatique et libertés.
▪ Elle a également publié en ligne des **fiches pratiques**, des outils et des codes sources à destination des professionnels, ainsi qu'une vidéo pédagogique et des fiches conseils permettant de limiter la traçabilité d'une navigation sur le net.
▪ Enfin, elle a mis à la disposition des internautes la **version 1.0 de Cookieviz**, un logiciel développé par les experts de la Cnil permettant la visualisation en temps réel du dépôt et de la lecture des cookies.
▪ Ce logiciel peut être téléchargé gratuitement depuis le compte Source Forge de la Commission (1).

(1) Cnil, rubrique Actualités, art. du 16-12-2013

Télécharger Cookieviz

L'impact des drones sur les libertés individuelles et le respect de la vie privée

▪ La **sixième Lettre innovation et prospective**, publiée par la Cnil en décembre, comporte un dossier sur le développement des drones et ses incidences en termes d'innovation, de respect de la vie privée et de protection des libertés individuelles.
▪ Une **interview du professeur Ryan Calo** de l'Université de Washington figure également dans la lettre, dans laquelle il fait état de ses travaux sur les drones, la robotique et la vie privée.

(2) Cnil, Lettre n°6 12-2013

L'Autorité monégasque de protection des données personnelles fête ses 20 ans

▪ La Commission de contrôle des informations nominatives (**CCIN**), autorité administrative indépendante instituée par la loi n° 1.165 du 23 décembre 1993, fête ses vingt ans.
▪ Elle publie, à cette occasion, une bande dessinée pédagogique destinée à présenter, de manière ludique, les thématiques propres à la protection des données personnelles (3).

(3) CCIN, rubrique Actualités

Protection des données personnelles : 7ème conférence de l'AFAPDP

▪ La 7ème conférence sur la protection des données personnelles s'est déroulée les **21 et 22 novembre 2013** à Marrakech (Maroc).
▪ Instituée par l'Association francophone des autorités de protection des données personnelles (AFAPDP), en concertation avec l'Organisation internationale de la Francophonie (OIF) et la Commission nationale de contrôle de la protection des données à caractère personnel (CNDP) du Maroc, elle a permis aux autorités de régulation d'échanger sur les principales problématiques intéressant la protection des données (4).

(4) Site de l'AFAPDP

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/

COMMERCE ELECTRONIQUE : QUESTIONS SUR LE TRAITEMENT DES DONNEES RELATIVES A LA CARTE DE PAIEMENT

Les consommateurs sont-ils informés de l'utilisation du numéro de leur carte de paiement ?

Référence

▪ **Oui**, toute utilisation du numéro de carte de paiement, quelle qu'en soit la finalité, doit faire l'objet d'une **information complète et claire du titulaire de la carte** (1).

▪ Il doit ainsi avoir connaissance :

- de l'identité du responsable du traitement ;
- des finalités du traitement ;
- du caractère obligatoire ou facultatif des informations à renseigner ;
- des conséquences éventuelles, à leur égard, d'un défaut de réponse ;
- de l'identité des destinataires des données ;
- de l'existence et les modalités d'exercice du droit d'accès, de rectification et d'opposition au traitement de données et le cas échéant des transferts de données hors Union européenne.

▪ Dans l'hypothèse où les données relatives à la personne ont été communiquées à un tiers par le commerçant, celui-ci doit informer ce tiers sans délai de l'exercice du droit d'opposition ou de rectification du titulaire de la carte de paiement.

(1) Cnil, Délib. 2013-358 du 14-11-2013.

Le traitement des données présente-t-il des garanties suffisantes en termes de sécurité ?

▪ **Oui**, le traitement des données présente des garanties suffisantes en termes de sécurité.

▪ Le responsable de traitement est **tenu de prendre des mesures de sécurité** afin d'éviter notamment tout accès illégitime aux données traitées. Ces mesures doivent être proportionnées aux risques engendrés par le traitement pour les personnes concernées (2).

▪ Les accès non autorisés aux données relatives à la carte pouvant déboucher sur la réalisation de transactions frauduleuses, la confidentialité de ces données se doit d'être spécifiquement protégée. Le non-respect de cette obligation de sécurité est sanctionné de cinq ans d'emprisonnement et de 300 000 euros d'amende (3).

▪ - Le responsable de traitement désirant externaliser la gestion du système de paiement doit choisir un sous-traitant présentant des garanties suffisantes permettant de s'assurer de la mise en œuvre des mesures de sécurité rendues nécessaires, et de fixer contractuellement les objectifs de sécurité qu'il impose à son sous-traitant (4).

▪ Dans tous les cas, le recours à la sous-traitance ne dispense en aucun cas le responsable de traitement de ses obligations au titre de l'article 34 de la loi Informatique et libertés.

▪ La Cnil, par délibération du 14 novembre 2013, préconise un renforcement des exigences sécuritaires.

▪ Elle recommande notamment :

- d'utiliser uniquement des dispositifs conformes à des référentiels reconnus en matière de sécurisation de données au niveau européen ou international (standard PCI DSS) ;
- de restreindre les accès au numéro de la carte de paiement des clients ;
- de mettre en œuvre des moyens d'authentification renforcée du titulaire de la carte ;
- d'instaurer des mesures de traçabilité spécifiques, lorsque les données relatives à la carte sont conservées afin de faciliter la réalisation ultérieure de transactions ;
- d'adresser une notification aux personnes dont les données ont fait l'objet d'une violation de sécurité afin qu'elles puissent prendre les mesures appropriées pour limiter les risques de réutilisation frauduleuse de leurs données (contestation de paiements frauduleux, mise en opposition de la carte, etc.).

(2) Loi 78-17 du 6-1-1978 modifiée, art. 34.

(3) C. pén. art 226-17

(4) Loi 78-17 du 6-1-1978 modifiée, art. 35

Prochains événements

Le renouveau de la signature électronique : 29 janvier 2014

▪ Eric Barbry, Polyanna Bigle co-animeront, avec Dimitri Mouton (société Demaeter), un petit-déjeuner débat dédié au renouveau de la signature électronique.
▪ Avec internet apparaissent de nouvelles formes de signatures qui se propagent dans les usages quotidiens. Des signatures effectuées sur tablettes électroniques, par courriel ou par d'autres moyens (QR code-code barre 2D), aux signatures à la volée ou éphémères proposées par les plateformes de signature en ligne, la signature électronique entre dans les mœurs.
▪ Autrefois réservée à des applications professionnelles, elle se déploie dans le grand public à une vitesse impressionnante avec l'e-commerce. De nombreuses plateformes proposent aux entreprises de faire signer électroniquement tous types de documents à leurs correspondants professionnels ou particuliers et d'ajouter un bouton « Signer » à leur site Internet, de la même façon qu'un service de paiement en ligne. Il s'agit la plupart du temps d'un code à usage unique envoyé par sms sur le téléphone mobile de l'internaute afin de lui permettre d'accepter le document qu'il visualise.
▪ Ces solutions de contractualisation numérique font partie d'une stratégie multicanal BtoB et BtoC qui permet d'accélérer le développement commercial, en améliorant le taux de transformation.
▪ Ce petit-déjeuner sera l'occasion d'examiner les questions suivantes :

- Quelle est la valeur juridique des signatures à la volée ou sur tablette ?
- Quelle est la qualité des preuves électroniques ?
- Comment maîtriser les risques juridiques ?
- Comment rédiger une convention sur la preuve ?
- Qu'est-ce qu'un dossier de preuve ou un chemin de preuve ?
- Qu'y a-t-il concrètement derrière ces différentes formes de signature électronique ?

▪ **Inscription gratuite** sous réserve de confirmation avant le 27 janvier 2014 à l'aide du formulaire en ligne.

Elus locaux : comment protéger votre e-réputation ? 12 février 2014

▪ Virginie Bensoussan-Brulé et Claudine Salomon animeront un petit-déjeuner débat consacré à la protection par les élus locaux de leur e-réputation et du nom de leur commune.
▪ Usurpation d'identité, dénigrement, injure ou diffamation, citations hors contexte, comment lutter contre l'e-médisance des usagers mécontents et des adversaires politiques à quelques semaines des élections municipales ? Comment anticiper pour mieux réagir ?
▪ La viralité des réseaux sociaux et l'absence de droit à l'oubli sur internet impose une vigilance de chaque instant car il faut réagir très vite. Au-delà de la réputation des élus, les communes peuvent être, en ce qui les concerne, la cible de pratiques qui portent atteinte à leurs droits.
▪ Le projet de loi relatif à la consommation en cours de discussion va introduire, au bénéfice des collectivités territoriales et établissements intercommunaux, la possibilité de demander à l'Inpi à être alertés en cas de dépôt d'une demande d'enregistrement d'une marque incorporant leur nom. Les communes pourraient ainsi s'opposer à une telle demande avant d'être contraintes d'engager une procédure judiciaire coûteuse.
▪ Ce petit-déjeuner sera l'occasion d'examiner les questions suivantes :

- Quels sont les recours judiciaires pour gérer son e-réputation ?
- Comment intervenir auprès des hébergeurs et fournisseurs d'accès internet ?
- Comment le nom d'une commune est-il actuellement protégé par le droit ?
- Quelle est la position des tribunaux ?
- Quels sont les nouveaux dispositifs à venir et comment les mettre en œuvre ?

▪ **Inscription gratuite** sous réserve de confirmation avant le 10 février 2014 à l'aide du formulaire en ligne.

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