PROTECTION DES DONNÉES PERSONNELLES ET OBLIGATION DE SÉCURITÉ : LE POINT SUR LES NOUVEAUTÉS

Thiébaut DEVERGRANNE
Docteur en droit
Consultant

Paris – 3 avril 2012

Introduction

Qui suis-je ?

- Consultant - droit des nouvelles technologies
- +10 ans d'expérience, dont 6 pour les services du Premier ministre (SGDN/DCSSI) en qualité de conseil juridique
- Docteur en droit privé sciences criminelles
- Formation d'avocat (CAPA)
- Passionné de nouvelles technologies - programmation / sysadmin depuis +15 ans

http://www.donneespersonnelles.fr

Des nouveautés ?

- Ordonnance 24 août 2011 – art. 34 bis
- Proposition de loi DÉTRAIGNE / ESCOFFIER visant à mieux garantir le droit à la vie privée à l'heure du numérique
- Proposition de règlement européen 25 janvier 2012
  - Impact (business) sur la SSI
- Influence importante du respect de l'obligation de sécurité sur le développement de la SSI
  - Comprendre les vecteurs d'application de l'obligation de sécurité
  - Mécanisme d'influence
  - Business drive (ex : audit informatique et libertés)

Plan

- I - La protection des données personnelles en 2012
  - Un bilan très mitigé
  - La réaction : le projet de règlement européen
- II - L'obligation de sécurité et les changements récents
  - L'obligation de sécurité
  - L'obligation de notification
- III - Anticiper les changements à venir
  - La notification
  - L'obligation de sécurité & l'étude d'impact

I - La protection des données personnelles en 2012

Un bilan très mitigé…

All Complaints against Facebook Ireland Ltd.

no	date	topic	status	files
01	18-AUG-2011	**Pokes.** Pokes are kept even after the user "removes" them.	Filed with the Irish DPC	Complaint (PDF) Attachments (ZIP)
02	18-AUG-2011	**Shadow Profiles.** Facebook is collecting data about people without their knowledge. This information is used to substitute existing profiles and to create profiles of non-users.	Filed with the Irish DPC	Complaint (PDF) Attachments (ZIP)
03	18-AUG-2011	**Tagging.** Tags are used without the specific consent of the user. Users have to "untag" themselves (opt-out). *Info: Facebook announced changes.*	Filed with the Irish DPC	Complaint (PDF) Attachments (ZIP)
04	18-AUG-2011	**Synchronizing.** Facebook is gathering personal data e.g. via its iPhone-App or the "friend finder". This data is used by Facebook without the consent of the data subjects.	Filed with the Irish DPC	Complaint (PDF) Attachments (ZIP)
05	18-AUG-2011	**Deleted Postings.** Postings that have been deleted showed up in the set of data that was received from Facebook.	Filed with the Irish DPC	Complaint (PDF) Attachments (ZIP)
06	18-AUG-2011	**Postings on other Users' Pages.** Users cannot see the settings under which content is distributed that they post on other's pages.	Filed with the Irish DPC	Complaint (PDF) Attachments (ZIP)
07	18-AUG-2011	**Messages.** Messages (incl. Chat-Messages) are stored by Facebook even after the user "deleted" them. This means that all direct communication on Facebook can never be deleted.	Filed with the Irish DPC	Complaint (PDF) Attachments (ZIP)
08	18-AUG-2011	**Privacy Policy and Consent.** The privacy policy is vague, unclear and contradictory. If European and Irish standards are applied, the consent to the privacy policy is not valid.	Filed with the Irish DPC	Complaint (PDF) Attachments (ZIP)
09	18-AUG-2011	**Face Recognition.** The new face recognition feature is an inproportionate violation of the users right to privacy. Proper information and an unambiguous consent of the users is missing.	Filed with the Irish	Complaint (PDF) Attachments (ZIP)

Il en résulte :

Points communs entre CIL et RSSI ?

Ils éprouvent les mêmes difficultés pour…

- être impliqués en amont
- faire passer l'idée que « mieux vaut prévenir que guérir »
- sensibiliser utilisateurs et direction
- faire appliquer les décisions, politiques, charte, etc.
- contrôler, (faire) sanctionner, (inciter à) corriger
- s'engager auprès de leur direction sur une obligation de résultats
- justifier leurs demandes de dépense (ROI sécurité ?)
- valoriser leurs actions (si pas d'incident, avions nous réellement besoin de faire des efforts ?)

Ils sont également ressentis/perçus comme

- des « improductifs »
- des « empêcheurs de tourner en rond »

Mais le CIL a la loi pour lui…

AFCDP

www.afcdp.net

Extrait de la présentation de Bruno Rasle- Délégué Général AFCDP - à l'Ossir - 2009

Pas d'exploitation légale sans conformité CNIL…

Firewall ?

IPS / DPL / contrôle interne

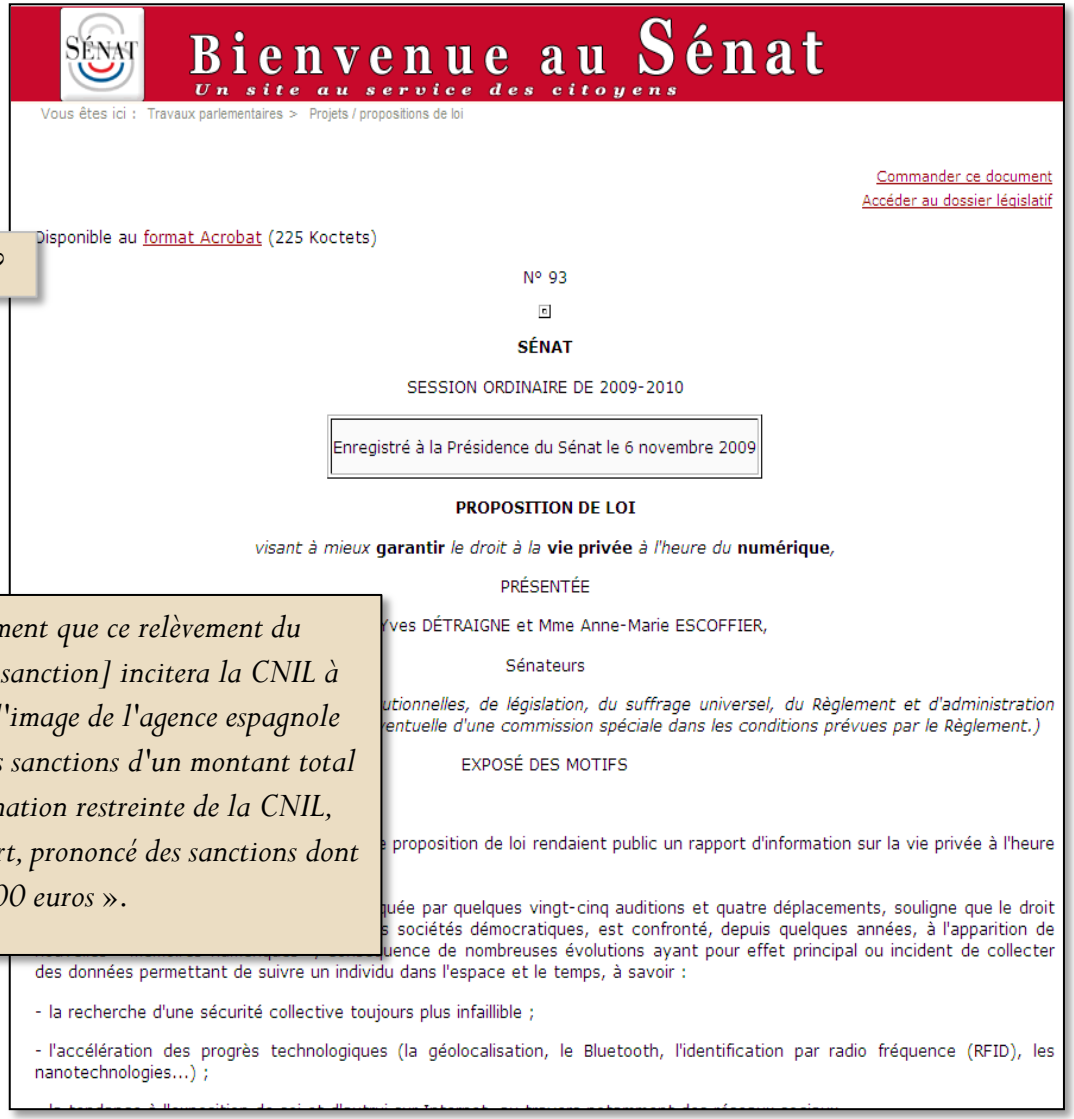
La protection des données personnelles en 2012

Le régulateur réagit…

La protection des données personnelles en 2012

L'avenir de la loi informatique et libertés ?

« Les auteurs de la proposition de loi estiment que ce relèvement du plafond légal [jusqu'à 600.000 euros de sanction] incitera la CNIL à faire preuve d'une plus grande fermeté, à l'image de l'agence espagnole qui, sur la seule année 2008, a infligé des sanctions d'un montant total de 22,6 millions d'euros alors que la formation restreinte de la CNIL, depuis sa création en 2005, a, pour sa part, prononcé des sanctions dont le montant cumulé ne s'élève qu'à 520.400 euros ».



Bienvenue au Sénat

Un site au service des citoyens

Vous êtes ici : Travaux parlementaires > Projets / propositions de loi

Commander ce document

Accéder au dossier législatif

Disponible au format Acrobat (225 Koctets)

N° 93

SÉNAT

SESSION ORDINAIRE DE 2009-2010

Enregistré à la Présidence du Sénat le 6 novembre 2009

PROPOSITION DE LOI

visant à mieux **garantir** *le droit à la* **vie privée** *à l'heure du* **numérique**,

PRÉSENTÉE

Yves DÉTRAIGNE et Mme Anne-Marie ESCOFFIER,

Sénateurs

utionnelles, de législation, du suffrage universel, du Règlement et d'administration ventuelle d'une commission spéciale dans les conditions prévues par le Règlement.)

EXPOSÉ DES MOTIFS

e proposition de loi rendaient public un rapport d'information sur la vie privée à l'heure

quée par quelques vingt-cinq auditions et quatre déplacements, souligne que le droit s sociétés démocratiques, est confronté, depuis quelques années, à l'apparition de uence de nombreuses évolutions ayant pour effet principal ou incident de collecter des données permettant de suivre un individu dans l'espace et le temps, à savoir :

- la recherche d'une sécurité collective toujours plus infaillible ;

- l'accélération des progrès technologiques (la géolocalisation, le Bluetooth, l'identification par radio fréquence (RFID), les nanotechnologies...) ;

Projet de règlement européen…

Art. 79 :
Sanctions : 2% du CA global d'un groupe

A 2% annual turnover fine would have meant 1.2 Billion dollars in 2008 for a company like Microsoft !

http://www.donneespersonnelles.fr

Effet de levier important vital pour le respect de l'obligation de sécurité !

II - L’obligation de sécurité et ses changements récents

Art. 226-17 c .pen. : « Le fait de procéder ou de faire procéder à un traitement de données à caractère personnel sans mettre en œuvre les mesures prescrites à l'article 34 de la loi n° 78-17 du 6 janvier 1978 précitée, est puni de cinq ans d'emprisonnement et de 300 000 EUR d'amende ».

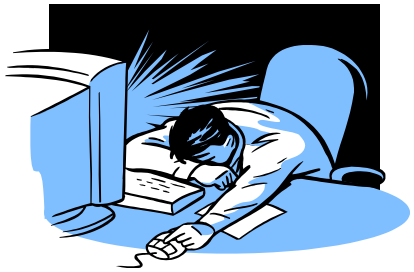
Article 34

Le responsable du traitement est tenu de prendre toutes précautions utiles, au regard de la nature des données et des risques présentés par le traitement, pour préserver la sécurité des données et, notamment, empêcher qu'elles soient déformées, endommagées, ou que des tiers non autorisés y aient accès.

« C'est une obligation de moyens ! »

L’obligation de sécurité et ses changements récents

Et la nouvelle obligation de notification…



Ordonnance 24 août 2011

Article 34 bis

I. - Le présent article s'applique au traitement des données à caractère personnel mis en œuvre dans le cadre de la fourniture au public de services de communications électroniques sur les réseaux de communications électroniques ouverts au public, y compris ceux prenant en charge les dispositifs de collecte de données et d'identification.

Pour l'application du présent article, on entend par violation de données à caractère personnel 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.

II. - En cas de violation de données à caractère personnel, le fournisseur de services de communications électroniques accessibles au public avertit, sans délai, la Commission nationale de l'informatique et des libertés.

Lorsque cette violation peut porter atteinte aux données à caractère personnel ou à la vie privée d'un abonné ou d'une autre personne physique, le fournisseur avertit également, sans délai, l'intéressé.

La notification d'une violation des données à caractère personnel à l'intéressé n'est toutefois pas nécessaire si la Commission nationale de l'informatique et des libertés a constaté que des mesures de protection appropriées ont été mises en œuvre par le fournisseur afin de rendre les données incompréhensibles à toute personne non autorisée à y avoir accès et ont été appliquées aux données concernées par ladite violation.

A défaut, la Commission nationale de l'informatique et des libertés peut, après avoir examiné la gravité de la violation, mettre en demeure le fournisseur d'informer également les intéressés.

III. - Chaque fournisseur de services de communications électroniques tient à jour un inventaire des violations de données à caractère personnel, notamment de leurs modalités, de leur effet et des mesures prises pour y remédier et le conserve à la disposition de la commission.

Anticiper les changements

III - Anticiper les changements

Anticiper les changements

- Projet de règlement européen
  - Notification à l'autorité de contrôle des violations de données personnelles (art. 30)
    - Concerne tout le monde, pas seulement les OCE
    - « Sans retard injustifié »
    - « Si possible 24 heures au plus tard »
    - Justification si +24h.
  - Le sous-traitant doit informer le responsable du traitement de toute violation qu'il connait
  - La notification décrit
    - Nature des données, nb personnes concernées
    - Point de contact
    - Mesures d'atténuation
    - Conséquences de la violation
    - Mesures ayant été prises pour y remédier

Article 30

1. En cas de violation de données à caractère personnel, le responsable du traitement en adresse notification à l'autorité de contrôle sans retard injustifié et, si possible, 24 heures au plus tard après en avoir pris connaissance. Lorsqu'elle a lieu après ce délai de 24 heures, la notification comporte une justification à cet égard.
2. En vertu de l'article 26, paragraphe 2, point f), le sous-traitant alerte et informe le responsable du traitement immédiatement après avoir constaté la violation de données à caractère personnel.
3. La notification visée au paragraphe 1 doit, à tout le moins:
a) décrire la nature de la violation de données à caractère personnel, y compris les catégories et le nombre de personnes concernées par la violation et les catégories et le nombre d'enregistrements de données concernés;
b) communiquer l'identité et les coordonnées du délégué à la protection des données ou d'un autre point de contact auprès duquel des informations supplémentaires peuvent être obtenues;
c) recommander des mesures à prendre pour atténuer les éventuelles conséquences négatives de la violation de données à caractère personnel;
d) décrire les conséquences de la violation de données à caractère personnel;
e) décrire les mesures proposées ou prises par le responsable du traitement pour remédier à la violation de données à caractère personnel.

- Projet de règlement européen
  - Le responsable conserve une trace documentaire de toute violation
    - Contexte
    - Effets
    - Mesures mises en œuvre pour y remédier

Article 30 (suite)

Le responsable du traitement conserve une trace documentaire de toute violation de données à caractère personnel, en indiquant son contexte, ses effets et les mesures prises pour y remédier. La documentation constituée doit permettre à l'autorité de contrôle de vérifier le respect des dispositions du présent article. Elle comporte uniquement les informations nécessaires à cette fin.

5. La Commission est habilitée à adopter des actes délégués en conformité avec l'article 86, aux fins de préciser davantage les critères et exigences applicables à l'établissement de la violation de données visée aux paragraphes 1 et 2 et concernant les circonstances particulières dans lesquelles un responsable du traitement et un sous-traitant sont tenus de notifier la violation de données à caractère personnel.

6. La Commission peut définir la forme normalisée de cette notification à l'autorité de contrôle, les procédures applicables à l'obligation de notification ainsi que le formulaire type et les modalités selon lesquelles est constituée la documentation visée au paragraphe 4, y compris les délais impartis pour l'effacement des informations qui y figurent. Les actes d'exécution correspondants sont adoptés conformément à la procédure d'examen prévue à l'article 87, paragraphe 2.

Anticiper les changements

- Projet de règlement européen
  - Communication de la violation **à la personne concernée**
    - Sans retard indu
    - Description précise de la violation
  - Dans certains cas, la communication peut être écartée avec l'aval de l'autorité nationale de contrôle
    - Nécessite que les mesures de protection sont mises en œuvre

Art 32

1. Lorsque la violation de données à caractère personnel est susceptible de porter atteinte à la protection des données à caractère personnel ou à la vie privée de la personne concernée, le responsable du traitement, après avoir procédé à la notification prévue à l'article 31, **communique la violation sans retard indu à la personne concernée.**
2. La communication à la personne concernée prévue au paragraphe 1 décrit la nature de la violation des données à caractère personnel et contient au moins les informations et recommandations prévues à l'article 31, paragraphe 3, points b) et c).
3. La communication à la personne concernée d'une violation de ses données à caractère personnel n'est pas nécessaire si le responsable du traitement prouve, à la satisfaction de l'autorité de contrôle, qu'il a mis en œuvre les mesures de protection technologiques appropriées et que ces dernières ont été appliquées aux données concernées par ladite violation. De telles mesures de protection technologiques doivent rendre les données incompréhensibles à toute personne qui n'est pas autorisée à y avoir accès.
4. Sans préjudice de l'obligation du responsable du traitement de communiquer à la personne concernée la violation de ses données à caractère personnel, si le responsable du traitement n'a pas déjà averti la personne concernée de la violation de ses données à caractère personnel, l'autorité de contrôle peut, après avoir examiné les effets potentiellement négatifs de cette violation, exiger du responsable du traitement qu'il s'exécute.

- **Projet de loi Detraigne/Escoffier**
  - Très similaire au projet de règlement européen
  - Notification CNIL
    - Via CIL, si CIL
    - Resp. prend immédiatement les mesures nécessaires
  - Notification des personnes concernées
    - Attention aucune exception prévue dans la loi française!

Article 7

L'article 34 de la loi n° 78-17 du 6 janvier 1978 précitée est ainsi rédigé : (…)

« En cas de violation du traitement de données à caractère personnel, le responsable de traitement **avertit sans délai le correspondant "informatique et libertés"** ou, en l'absence de celui-ci**, la Commission nationale de l'informatique et des libertés**. Le responsable du traitement, avec le concours du correspondant "informatique et libertés", prend immédiatement les mesures nécessaires pour permettre le rétablissement de la protection de l'intégrité et de la confidentialité des données. Le correspondant "informatique et libertés" en informe la Commission nationale de l'informatique et des libertés. Si la violation a affecté les données à caractère personnel d'une ou de plusieurs personnes physiques, le responsable du traitement en informe également ces personnes, sauf si ce traitement a été autorisé en application de l'article 26. Le contenu, la forme et les modalités de cette information sont déterminés par décret en Conseil d'État pris après avis de la Commission nationale de l'informatique et des libertés. Un inventaire des atteintes aux traitements de données à caractère personnel est tenu à jour par le correspondant "informatique et libertés".

« Des décrets, pris après avis de la Commission nationale de l'informatique et des libertés, peuvent fixer les prescriptions techniques auxquelles doivent se conformer les traitements mentionnés aux 2° et 6° du II de l'article 8. »

A retenir…

- Préparez-vous dès maintenant à…
  - Tracer précisément les incidents de sécurité ayant un impact sur des données personnelles
    - Au sein de l'entreprise
    - Auprès de vos sous-traitants
  - Savoir comment gérer une remontée des incidents et information CNIL en 24h ?
  - Tester l'impact de la notification sur la continuité business
- Suivre l'évolution du projet de règlement qui impose formellement l'analyse de risques SSI
  - Impact business!

Conclusion

Questions ?

Thiébaut DEVERGRANNE

Contact : td@hstd.net

http://www.donneespersonnelles.fr