Information Security Breaches & The Law

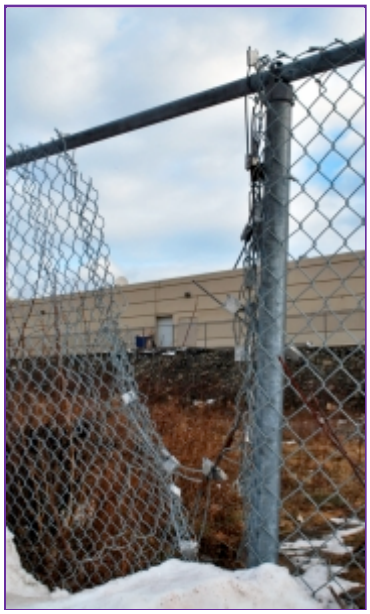
Type here and press enter t

- Home
- About »
- "Security Breaches" Library

La France va-t-elle se doter d'une loi rendant obligatoire les notifications des violations de sécurité ?

Posted by "Security Breaches" Administrator on 03/08/2010 · Leave a Comment

La proposition de loi *visant à mieux garantir le droit à la vie privée à l'heure du numérique*, présentée le 6 novembre 2009 au Sénat par les sénateurs Yves Détraigne et Anne-Marie Escoffier, a été adoptée par le Sénat et transmise à l'Assemblée nationale le 24 mars 2010. (Historique de la législation.) Elle devrait à nouveau être débattue à l'automne.



"Security Breach" (Armdale, Halifax, Nova Scotia, Canada) - Photo by: meddygarnet (2010)

Une proposition de loi qui transpose la Directive européenne 2009/136/CE

Cette proposition de loi anticipait la publication le 25 novembre 2009 de la Directive 2009/136/CE

modifiant la Directive 2002/58/CE "vie privée et communications électroniques". Son article 2 (c) ajoute une obligation de notifier les violations de sécurité à « l'autorité nationale compétente » et aux personnes concernées par cette faille de sécurité, du moins si cette faille est *"de nature à affecter négativement"* leurs données à caractère personnel.

> *"En cas de violation de données à caractère personnel, le fournisseur de services de communications électroniques accessibles au public avertit sans retard indu l'autorité nationale compétente de la violation.*
>
> *Lorsque la violation de données à caractère personnel est de nature à affecter négativement les données à caractère personnel ou la vie privée d'un abonné ou d'un particulier, le fournisseur avertit également sans retard indu l'abonné ou le particulier concerné de la violation.*"

Cette Directive doit être transposée par les États membres au plus tard le 25 mai 2011. (Article 4 de la Directive.)

L'article 7 de la proposition de loi actuellement examinée par l'Assemblée nationale modifie l'article 34 de la loi no. 78-17 du 6 janvier 1978 et rend obligatoire, pour les responsables de traitements de données à caractère personnel, d'informer le correspondant "informatique et libertés" ou, en l'absence de celui-ci, la Commission nationale de l'informatique et des libertés (CNIL), d'une violation de l'intégrité ou de la confidentialité de ces traitements, ainsi que les personnes concernées par cette violation, sauf s'il s'agit d'un traitement autorisé en application de l'article 26, c'est-à-dire d'un fichier de police.

> *"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'.*
>
> *Le responsable du traitement met en œuvre toutes mesures adéquates, au regard de la nature des données et des risques présentés par le traitement, pour assurer la sécurité des données et en particulier protéger les données à caractère personnel traitées contre toute violation entraînant accidentellement ou de manière illicite la destruction, la perte, l'altération, la divulgation, la diffusion, le stockage, le traitement ou l'accès non autorisés ou illicite."*

Tel qu'il est actuellement rédigé, l'article 34 de la loi no. 78-17 du 6 janvier 1978 dispose simplement que

> "l*e 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".*

Le responsable a une obligation de mettre en oeuvre des mesures de sécurité, mais non de notifier d'éventuelles violations de sécurité.

La proposition de loi ne précise pas comment vérifier la sécurité des données

Selon le rapport du Sénateur Christian Cointat fait au nom de la commission des lois du Sénat, le but de l'obligation de notification, nouvelle en droit français, est d'inciter les responsables de traitement à mettre en œuvre des mesures de protection adéquates. (p. 16) Ce n'est pas tâche facile : le rapport d'information d'Yves Détraigne et d'Anne-Marie Escoffier sur le respect de la vie privée à l'heure du numérique, publié en mai 2009, notait que "*la sécurité des données est* ***en pratique difficile à vérifier****, à moins de contrôler chaque système de sécurité par des attaques-test*". (p. 99 du rapport) [en gras dans le texte]

Pourtant, bien que la sécurité des données soit "*difficile à vérifier*", la proposition de loi ne précise pas quelles pourraient être les mesures adéquates pour la protéger. La délibération de la CNIL n°81-94 du 21 juillet 1981 relative aux mesures générales de sécurité des systèmes informatiques recommandait déjà la mise en place de telles mesures de sécurité, qui seraient :

1. Une évaluation des risques et une étude générale de la sécurité systématique pour tous les traitements informatiques;
2. Un effort d'information et de sensibilisation auprès des catégories professionnelles concernées afin de les inciter à participation à l'application des mesures de sécurité;
3. Une définition particulièrement soignée des dispositions destinées à assurer la sécurité et la confidentialité des traitements et des informations, qui doivent être consignées dans un document de référence, tenu jour et dont il convient de veiller de manière permanente à son respect;
4. Une définition claire des responsabilités des personnels participant au respect des mesures de sécurité.

La proposition de loi ne prévoit pas non plus l'obligation légale de garantir contractuellement la sécurité des données

Ces mesures de sécurité doivent en outre, selon la CNIL, par

> *"des actions concertées entre les pouvoirs publics, les groupements professionnels d'utilisateurs, les constructeurs, les ingéniéries et les fournisseurs de matériels et de logiciels concour[ir] à préciser les sécurités offertes, à les garantir contractuellement, et à œuvrer dans le sens d'une amélioration générale de la sécurité, qui doit être prise en considération dès la conception des produits matériels ou logiciels".*

Nous regrettons que les mesures de sécurité des données prises par les entreprises ne soient pas toujours clairement portées à la connaissance des usagers et des clients. C'est d'autant plus regrettable que la CNIL recommandait dès 1981 que de telles mesures soient garanties contractuellement. Pourtant, le considerant 25 de la Directive 2009/136/CE souhaite que

> "*le contrat avec le client devrait aussi préciser le type de mesure éventuelle que le fournisseur pourrait prendre afin de réagir à un incident ayant trait à la sécurité ou à l'intégrité ou de faire face à des menaces ou à des situations de vulnérabilité*".

Par contre, elle prévoit l'obligation de notifier les violations de sécurité aux particuliers

La proposition loi initiale présentée en novembre 2009 donnait uniquement à la CNIL le pouvoir d'exiger du responsable de traitement qu'il avertisse les personnes concernées par cette atteinte, "*si cette atteinte est de nature à affecter les données à caractère personnel d'une ou de plusieurs personnes physiques*".

La proposition de loi a été modifiée au cours des travaux parlementaires au Sénat, et son article impose désormais au responsable du traitement d'informer les personnes dont les données personnelles peuvent avoir été compromises par une violation de la sécurité des données, à moins qu'il ne s'agisse d'un fichier de police autorisé par l'article 26 de la loi Informatique et libertés.

La première des lois rendant obligatoire la notification d'une infraction aux données, ("*data breach*") le *California Security Breach Notification Act*, entrée en vigueur dès juillet 2003, a rendu obligatoire la notification des violations de sécurité aux consommateurs résidant en Californie, et non à une autorité administrative indépendante telle que la CNIL. La Californie a pourtant depuis 2000 une agence gouvernementale dédiée à la protection de la vie privée des consommateurs, le *California Office of Privacy Protection*.

> "*Any agency that owns or licenses computerized data that includes personal information shall disclose any breach of the security of the system following discovery or notification of the breach in the security of the data to any resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person.*" (Cal. Civ. Code § 1798.29(a))

Elle semble suivre également la recommandation de la Directive 2009/136/CE de notifier aux particuliers les violations de sécurité pour tous les secteurs, pas seulement celui des communications électroniques.

L'article 2(c) de la Directive 2009/136/CE prévoit une obligation pour le responsable de traitement d'informer l'abonné ou le particulier concerné par une violation de données à caractère personnel si cette violation "*est de nature à affecter négativement ses données à caractère personnel ou sa vie privée*". Le champ de cette directive ne concerne néanmoins que les fournisseurs de services de communications électroniques accessibles au public.

Il s'agit pourtant là d'une question d'intérêt général. Le considérant 59 de la Directive 2009/136/CE regrette que les exigences relatives à la notification des violations de données à caractère personnel figurant dans la Directive 2002/58/CE soient

> *"limitées aux violations de sécurité intervenant dans le secteur des communications électroniques*" alors que *"la notification des violations de sécurité traduit l'intérêt général des citoyens à être informés des violations de sécurité. (…) L'intérêt des utilisateurs à être informés ne se limite pas, à l'évidence, au secteur des communications électroniques, et il convient dès lors d'introduire de façon prioritaire, au niveau communautaire, des exigences de notification explicites et obligatoires, applicables à tous les secteurs."*

C'est pourquoi, selon le considérant 59, la Commission devrait prendre les mesures nécessaires afin que la Directive 2002/58/CE soit appliquée quels que soient le secteur ou le type de données concernés.

> Cette recommandation semble avoir été entendue par le législateur français. Le rapport du Sénateur Christian Cointat souligne la nécessité de promouvoir la diffusion d'une culture "Informatique et libertés", dont l'un des points serait de rendre obligatoire les notifications des failles de sécurité, quel que soit le secteur ou le type de données concernés par la violation, avec la seule exception des données contenues dans les fichiers de police. (p. 16)

Affaire à suivre…

Un amendement déposé en février 2010 par le gouvernement devant le Sénat proposait de supprimer entièrement l'article 7. Le gouvernement arguait que cet article transposait la Directive 2009/136/CE de manière incomplète. En effet, selon le gouvernement, l'article 7 ne transpose pas les dispositions de cette directive relatives aux sanctions qui pourraient être prononcées contre le responsable de traitement qui n'aurait pas informé les personnes concernées par la faille de sécurité, ni les dispositions relatives à l'obligation pour le responsable du traitement de tenir un inventaire des violations de données à caractère personnel constatées. Cette obligation d'inventaire fut votée par le Sénat, sans toutefois voter l'amendement du gouvernement qui souhaitait la suppression totale de l'article 7 de la proposition de loi.

Nous ajoutons que la proposition de loi ne transpose pas la disposition de l'article 2 (4) (c) de la Directive 2009/136/CE selon laquelle il n'est pas nécessaire pour le fournisseur de notifier l'abonné d'une violation des données à caractère personnel si le fournisseur *"a prouvé, à la satisfaction de l'autorité compétente, 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 rendent les données incompréhensibles à toute personne qui n'est pas autorisée à y avoir accès."*

Il sera intéressant de suivre à l'automne le cheminement de la proposition de loi devant l'Assemblée nationale, pour autant qu'elle inscrive les débats sur cette proposition de loi à son calendrier.

Marie-Andrée Weiss & Cédric Laurant

Possibly related posts: (automatically generated)

- US-China: Le Grande Refroidissement
- Les PMEs innovantes ou leaders sur leur marché sont très exposées
- Le fichier Périclès, grand mix de données personnelles – Technologies …

Filed under Comments, FRANÇAIS · Tagged with CNIL, proposition de loi, droit à la vie privée, loi no. 78-17 du 6 janvier 1978, loi "Informatique et libertés", Assemblée nationale française, Sénat français, France, correspondant "informatique et libertés", Commission nationale de l'informatique et des libertés, confidentialité des données, sécurité des données, responsable du traitement, données à caractère personnel, accès non autorisé, mesures générales de sécurité des systèmes informatiques, délibération de la CNIL, California Security Breach Notification Act, délibération de la CNIL n°81-94 du 21 juillet 1981, California Office of Privacy Protection, violations de sécurité, Directive européenne 2002/58/CE, Directive européenne 2009/136/CE, Etats-Unis, Californie

Article 29 Data Protection Working Party reports on implementation of Data Retention Directive

Leave a Reply

Your email address will not be published. Required fields are marked *

Name *

Email *

Website

Comment

You may use these HTML tags and attributes: `<a href="" title=""> <abbr title=""> <acronym title=""> <b> <blockquote cite=""> <cite> <code> <pre> <del datetime=""> <em> <i> <q cite=""> <strike> <strong>`

Post Comment

Notify me of follow-up comments via email.

Subscribe by email to this site

- **Recent Posts**

- La France va-t-elle se doter d'une loi rendant obligatoire les notifications des violations de sécurité ?
- Article 29 Data Protection Working Party reports on implementation of Data Retention Directive
- Are 'clouds' located outside the European Union unlawful?
- The Safe Harbor Framework: not a "safe harbor" anymore for US companies? German expert body insists on stronger compliance stance
- Canada May Soon Have a Data Breach Law

- **Recent News on Security Breaches**

  - "Consumer View: Staying Safe from Cyber Snoops" (FCC, June 11, 2010) Recent news reports have focused attention on a growing concern: The ways in which wireless and WiFi networks can make consumers' private data accessible. (…)
  - "Sécurité des données personnelles : les entreprises ne font pas face" (ITR News, 9 juin 2010) L'étude souligne le fait que, en dépit de ce que croient beaucoup d'entreprises, le fait de respecter la réglementation en vigueur ne suffit pas à assurer une protection efficace des données. En effet, alors que 70 % des sondés affirment (…)
  - "Twitter Settles Charges that it Failed to Protect Consumers' Personal Information; Company Will Establish Independently Audited Information Security Program" (FTC, June 24, 2010) The FTC's complaint against Twitter charges that serious lapses in the company's data security allowed hackers to obtain unauthorized administrative control of Twitter, including access to non-public user information, tweets that consumers had (…)
  - "UK headed for data breach disclosure law within four years" (siliconcom, July 16, 2010) "According to lawyers at law firm Field Fisher Waterhouse, legislation requiring organisations to notify the relevant authorities as well as individuals affected in the event of a serious security breach will be introduced across Europe."
  - "Survey: 87 per cent of UK businesses favour mandatory disclosure of data breaches" (Secure Business Intelligence, July 6, 2010) 87 per cent of organisations believe that data breaches should be revealed when sensitive data about the public is exposed. Revealed, but to whom?
  - "Putting a Private Detective in Your Laptop" (New York Times, June 16, 2010) "According to a study by the Ponemon Institute, 12,000 laptops are lost each week in American airports (…) You can keep an eye on your devices and not leave them visible and unattended, but they might best be protected with some software."
  - "Credit Card Hackers Visit Hotels All Too Often" (New York Times, July 5, 2010) Hotels are a favorite target of hackers. A study released this year by data-security consulting company SpiderLabs found that "38 % of the credit card hacking cases last year involved the hotel industry".
  - Ponemon Institute: First Annual Cost of Cyber Crime Study (ArcSight, July 26, 2010) "The purpose of this benchmark study is twofold. First, we wanted to quantify the economic impact of a cyber attack. Second, we believed a better understanding of the cost of cyber crime will assist organizations in determining the appropriate amount (…
  - Rite Aid Settles FTC Charges That It Failed to Protect Medical and Financial Privacy of Customers and Employees (FTC, July 27, 2010) "The FTC began its investigation following news reports about Rite Aid pharmacies using open dumpsters to discard trash

that contained consumers' personal information such as pharmacy labels and job applications. (…)"

- **Tag Cloud**

adequate level of data protection Article 29 Data Protection Working Party Binding corporate rules Bundesdatenschutzgesetz C-29 Canada cloud computing confidentiality contractual clauses damage to reputation data breach notification statute data security Düsseldorfer Kreis encryption EU Directive 95/46/EC European Commission European data protection authorities European Union external audit Facebook German Federal Data Protection Act Germany identity theft integrity material breach online reputation personal data PIPEDA preemption Privacy Commissioner of Canada profile building companies reputation Safe Harbor Framework Safe Harbor self-certification search engines security breach security breach disclosure security breach notification self-regulation sensitive information sensitive personal information significant harm social networking sites TJX United States

- **Blog Authors**

- **Disclaimer & Comments Policy**

- Disclaimer & Comments Policy

- **Authors' upcoming talks & conferences on information security & legal issues**

  - Cédric Laurant: II Congresso Crimes Eletrônicos e formas de proteção (2nd Congress on Cybercrimes and Protection Measures) Federação do Comércio do Estado de São Paulo (Sao Paulo Chamber of Commerce), Sao Paulo, Brazil – Sept. 27-28, 2010
  - Cédric Laurant: "Legal Developments and Relevant Court Decisions in Latin America" High Technology Crime Investigation Association (HTCIA) International Conference (Atlanta, GA-USA – Sept. 20-22, 2010)

- **Tweets (last 10)**

  - La France va-t-elle se doter d'une loi rendant obligatoire les notifications des violations de sécurité ?: http://wp.me/pW5Fc-2G - tweeted 59 minutes ago
  - List of recent surveys and reports on security breaches: http://bit.ly/9VamhE - tweeted 5 days ago
  - ArcSight & Ponemon Institute: release of "1st Annual Cost of Cyber Crime Study" http://bit.ly/d1Us8e - tweeted 5 days ago
  - Article 29 Data Protection Working Party reports on implementation of Data Retention Directive. New blog posting at http://bit.ly/aOG3cY #in - tweeted 2 weeks ago
  - "Are 'clouds' located outside the European Union unlawful?" New blog posting. http://bit.ly/djUNCy #in - tweeted 2 weeks ago
  - "The Safe Harbor Framework: not a 'safe harbor' anymore for US Companies?" New blog posting. http://lnkd.in/ShwMWj - tweeted 3 weeks ago
  - "The Safe Harbor Framework: not a "Safe Harbor" anymore for US Companies?" New blog posting: http://wp.me/pW5Fc-1D - tweeted 3 weeks ago
  - FTC's proposed consent agreement with #Twitter: company misrepresented its security measures. http://bit.ly/cF8LNk - tweeted 1 month ago
  - Your "private" tweets are... public! #Twitter prone to security breaches, FTC says in consent agrmt. Com'ts requested. http://bit.ly/axKpnV - tweeted 1 month ago
  - FTC's 1st case agst social netwkg website: #Twitter failed to safeguard users' PII despite promises in privacy policy http://bit.ly/ajUG9J - tweeted 1 month ago

- **Subscribe to this blog by e-mail**

  Enter your e-mail address here to subscribe to this blog and receive notifications of new posts by e-mail.

  Sign me up!

-

- **Counters**

Information Security Breaches & The Law ·

Blog at WordPress.com. Theme: Structure by Organic Themes.