

## **Toutes les violations de données doivent être rendues publiques \***

*Peter Hustinx*

La bonne nouvelle, c'est que les législateurs européens souhaitent rendre obligatoire la divulgation des violations de données; la mauvaise, c'est que la loi ne s'appliquera pas à tous. Or, ces exemptions ne profitent à personne, affirme Peter Hustinx, le grand patron européen du respect de la vie privée.

Pas un jour ne passe sans que l'on prenne connaissance dans la presse de violations de la sécurité entraînant la perte de milliers, voire parfois de millions, de données. Le piratage de bases de données ou leur mauvais fonctionnement peut exposer les personnes à des usurpations d'identité, à des pertes financières et compromettre leur réputation en raison de la divulgation d'informations sensibles comme des numéros de cartes de crédit, des données bancaires ou médicales.

Lorsque de telles violations ont lieu, les personnes concernées devraient être averties afin de pouvoir entreprendre les démarches nécessaires. Hors d'Europe, des lois obligeant les organisations à avertir les personnes concernées ont déjà été adoptées; en fait, ces lois encouragent les sociétés à investir dans la sécurité afin d'éviter la mauvaise publicité que la divulgation de violations pourrait causer.

### **Gravité des conséquences**

En raison des graves conséquences qu'entraînent les violations de données, il est à espérer que les législateurs européens oseront introduire une obligation ferme d'avertir le consommateur en cas de violations susceptibles de porter atteinte à la vie privée.

La proposition visant à créer un mécanisme de signalement des violations de la sécurité, présentée par la Commission européenne et approuvée par le Parlement européen et le Conseil dans le cadre de la révision de la directive "vie privée et communications électroniques", devrait donc être bien accueillie par les citoyens et les acteurs européens en général.

Malheureusement, si l'approche du Conseil et de la Commission l'emporte, les citoyens européens seront déçus d'apprendre que les seules organisations obligées de divulguer les violations seront les fournisseurs de services de communications électroniques accessibles au public.

Cette restriction implique que les citoyens européens ne seront avertis que si leur fournisseur d'accès à Internet ou leur compagnie téléphonique est victime de violations de la sécurité. En revanche, si quelqu'un s'est introduit dans leur banque en ligne ou que le système de sécurité de cette dernière a été piraté, permettant ainsi à des personnes non autorisées d'avoir accès à des informations sur des comptes bancaires, il se peut que les citoyens ne soient pas avertis.

---

\* Article publié sur [ZDNet.co.uk](http://ZDNet.co.uk) le 29 janvier 2009.

Ainsi, à moins que les amendements proposés par le Parlement européen soient adoptés par le Conseil, les comptes et les autres activités économiques en ligne ne seront pas concernés.

Les raisons pour lesquelles le Conseil et la Commission adoptent une approche si restrictive ne sont pas totalement claires. La Commission base sa position sur des considérations d'ordre juridique: le champ d'application général de la directive "vie privée et communications électroniques" viserait uniquement les opérateurs de télécommunications et les fournisseurs d'accès.

Or, cette justification est contredite par l'existence d'autres sections de la directive, dont le champ est plus large. Étant donné l'ampleur des risques et la possibilité de les réduire en légiférant, il faut espérer que ces arguments qui ressortissent de la technique juridique n'empêcheront pas d'atteindre des objectifs aussi importants.

### **Informations sensibles**

En outre, le type d'informations généralement détenu par les banques, les fournisseurs de services de santé en ligne et les prestataires du commerce en ligne est sûrement au moins aussi sensible que celui qui est normalement traité par les fournisseurs de services de communications électroniques accessibles au public.

En effet, les personnes sont susceptibles de subir un préjudice en raison de la divulgation injustifiée tout autant de leurs données bancaires que de celles relatives à leurs appels téléphoniques, par exemple. Par conséquent, en raison du caractère sensible des informations concernées, il serait fortement conseillé d'élargir l'obligation de notification aux activités économiques en ligne.

Le bon sens et les avantages généraux pour les citoyens européens voudraient à l'évidence que les lois obligeant les organisations victimes de violations de données d'avertir les personnes concernées soient appliquées le plus largement possible: elles devraient inclure, au minimum, les prestataires du commerce en ligne et les fournisseurs de services de communications électroniques accessibles au public.

Comme la Commission européenne, le Parlement européen et le Conseil se concertent pour trouver une solution de compromis en vue de l'adoption finale de la directive "vie privée et communications électroniques", j'espère que les graves conséquences qu'engendre la violation de données les aideront à faire le bon choix.

*Peter Hustinx est le Contrôleur européen de la protection des données. Sa mission consiste à garantir la protection des personnes dont les données sont traitées par les institutions et les organes de la Communauté européenne, ainsi qu'à donner des avis sur les nouveaux textes législatifs ayant des implications pour la protection des données.*

