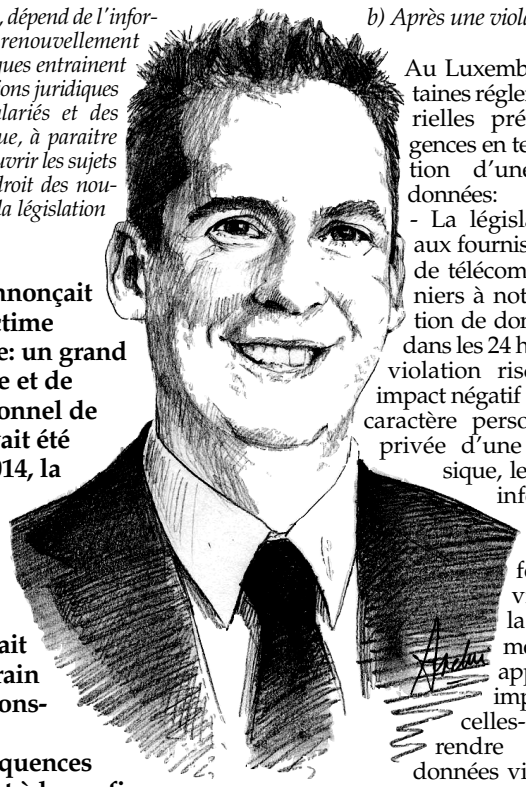
Chronique du droit des nouvelles technologies

Violation de données à caractère personnel – Que faire après l'affaire eBay ?

Toute entreprise, grande ou petite, dépend de l'informatique, domaine sujet à un renouvellement constant. Ces nouveautés techniques entrainent inévitablement de nouvelles questions juridiques impactant le quotidien des salariés et des employeurs. La présente rubrique, à paraitre tous les mois, a pour objectif de couvrir les sujets d'actualité et les évolutions en droit des nouvelles technologies au niveau de la législation luxembourgeoise et européenne.



En mai 2014, eBay annonçait qu'elle avait été victime d'une cyber-attaque: un grand nombre de mots de passe et de données à caractère personnel de nature non-financière avait été compromis. Le 27 mai 2014, la Commission Nationale pour la Protection des Données («CNDP»), en l'espèce compétente dès lors qu'eBay est établie au Luxembourg, annonçait ensuite qu'elle était en train d'investiguer sur les circonstances de la violation de données et sur ses conséquences par rapport à l'intégrité et à la confidentialité des données à caractère personnel des utilisateurs eBay dans l'UE.

eBay n'est qu'un nom de plus à s'ajouter sur une liste déjà longue d'acteurs de e-commerce et de plateformes en ligne victimes d'une attaque similaire. Néanmoins, il a ici été particulièrement reproché à eBay d'avoir mal géré la violation de données et de ne pas avoir adéquatement notifié ses clients. Le Président de la CNPD a d'ailleurs qualifié l'évènement de désastre mondial.

La question se pose alors de savoir s'il existe une meilleure façon de gérer une telle violation de données au Luxembourg. La réponse n'est pas évidente, dès lors que la loi luxembourgeoise en matière de protection des données à caractère personnel ne prévoit actuellement pas de cadre légal concernant la notification des violations de données. La situation pourrait néanmoins évoluer.

1. Le cadre légal luxembourgeois

a) Avant une violation de données

La loi modifiée du 2 août 2002 relative à la protection des personnes à l'égard du traitement de données à caractère personnel (la «loi sur la protection des données à caractère personnel») impose au «responsable du traitement» un certain nombre d'obligations. Ce dernier est défini comme la personne qui détermine les moyens et les finalités du traitement de données à caractère personnel.

En vertu de l'article 22 de ladite loi, le responsable du traitement doit mettre en œuvre toutes les mesures techniques appropriées pour éviter l'accès non-autorisé aux données et leur destruction accidentelle ou illicite. En outre, le responsable du traitement doit garder le contrôle sur ces mesures de sécurité et doit dès lors, s'il décide de sous-traiter les activités de traitement, choisir un sous-traitant qui apporte des garanties suffisantes au regard des mesures de sécurité.

L'article 23 précise que les mesures à utiliser dépendront du risque d'atteinte à la vie privée, ainsi que de l'état de l'art et du coût lié à la mise en œuvre de telles mesures. Ainsi, le responsable du traitement devra d'abord évaluer les risques liés au traitement et devra en principe procéder à une étude d'impact sur la vie privée. Il devra ensuite décider des différentes mesures de sécurité à implémenter.

Afin de s'assurer que chaque responsable du traitement respecte ces exigences, la CNPD peut demander la fourniture d'une description des mesures mises en place ou de tout changement majeur de celles-ci. L'entreprise dispose alors de 50 jours pour communiquer ces informations. Les responsables du traitement doivent ainsi s'assurer qu'ils disposent d'une documentation claire détaillant les mesures prises afin de pouvoir répondre rapidement à la requête de la CNPD.

En outre, la plupart des traitements de données doivent faire l'objet d'une notification générale auprès de la CNPD, dans laquelle les mesures de sécurité doivent être décrites de façon globale. Certains traitements critiques de données requièrent néanmoins une autorisation préalable de la CNPD (par exemple, le traitement des données résultant du monitoring de l'outil informatique), auquel cas une description plus détaillée des mesures de sécurité devra être fournie à la CNPD.

b) Après une violation de données

Au Luxembourg, seules certaines réglementations sectorielles prévoient des exigences en termes de notification d'une violation de données:

- La législation applicable aux fournisseurs de services de télécoms oblige ces derniers à notifier toute violation de données à la CNPD dans les 24 heures. Lorsque la violation risque d'avoir un impact négatif sur les données à caractère personnel ou la vie privée d'une personne physique, le fournisseur doit informer cette dernière sans retard excessif. Si le fournisseur parvient à prouver à la CNPD que des mesures de sécurité appropriées ont été implémentées et que celles-ci ont servi à rendre illisibles les données violées pour toute personne non autorisée à y accéder, le fournisseur ne devra pas notifier la violation à la personne concernée. Partant, les fournisseurs utilisant des moyens de cryptographie ne devront en principe pas notifier la violation de données aux personnes concernées.
- Conformément à la Circulaire 11/504 de l'autorité de surveillance du secteur financier («CSSF»), les établissements financiers ont le devoir de signaler les attaques IT dont ils sont la cible, spécifiquement lorsque celles-ci mènent à une violation de données.

La loi sur la protection des données à caractère personnel ne contient par contre pas de disposition contraignant les responsables de traitement à notifier la CNPD ou les personnes concernées en cas de violation de données. Il peut néanmoins être utile de notifier la violation à la CNPD (de manière informelle) ou aux personnes concernées, car:

- premièrement, la CNPD sera plus encline à travailler avec le responsable du traitement, si ce dernier fait preuve d'une volonté de remédier à tout dommage souffert par la personne concernée suite à la violation ;
- deuxièmement, conformément aux principes généraux du droit des contrats et de la responsabilité civile au Luxembourg, une personne qui cause un dommage à autrui a l'obligation d'adopter des mesures limitant le dommage. Cela signifie que lorsque le responsable du traitement a été victime d'une violation de données, il a l'obligation de notifier celle-ci aux personnes concernées, dès lors qu'une telle notification est de nature à limiter le dommage potentiel. Ceci est particulièrement vrai si des mots de passe ont fait l'objet de la fuite de données.

Une fois informée d'une violation, ou en cas de soupçon d'une telle violation, la CNPD peut investiguer les activités de traitement du responsable du traitement. Selon l'article 32 de la loi sur la protection des données à caractère personnel, la CNPD a ainsi le droit de réaliser les contrôles nécessaires afin de s'assurer que le responsable du traitement se conforme aux exigences en matière de protection des données. Cela veut dire que la CNPD dispose d'un accès direct aux locaux du responsable du traitement. Dans l'affaire eBay, la CNPD va par exemple contrôler les mesures de sécurité que l'entreprise avait mises en place et évaluer leur efficacité.

Contrairement à plusieurs autres autorités nationales, la CNPD ne dispose pas de pouvoir de sanction financière. Néanmoins, l'article 33 de la loi sur la protection des données à caractère personnel lui donne le pouvoir de prononcer des sanctions administratives, telles que l'interdiction, définitive ou temporaire, de procéder à un traitement de donner, ou un ordre de publication de la décision. Qu'elle soit définitive ou temporaire, l'interdiction empêchera certainement le responsable du traitement d'exercer effectivement son activité.

De plus, la CNPD ou les personnes concernées peuvent déférer l'affaire aux autorités pénales. En vertu de l'article 25 de la loi sur la protection des données à caractère personnel, le responsable du traitement peut être condamné à une peine de prison de 8 jours à 6 mois et/ou à une amende de 251 à 125.000 euros s'il s'avère qu'il n'a pas mis en place des mesures de sécurité suffisantes. Dès lors, même si la CNPD ne dispose pas de pouvoirs directs de sanctionner financièrement, les responsables du traitement peuvent néanmoins se voir infliger une amende.

2. Initiatives européennes

a) La proposition de règlement relatif à la protection des données

Actuellement en cours d'élaboration, la proposition de règlement relatif à la protection des données (COM (2012) 11) telle qu'approuvée par le Parlement Européen («PE») prévoit également une obligation de notifier les violations de données. Elle oblige tous les responsables du traitement à notifier toute violation à l'autorité nationale de protection des données sans délai injustifié.

Le responsable du traitement devra ensuite communiquer la violation de données aux personnes concernées sans délai injustifié, dès lors que la violation est susceptible de porter atteinte à la protection des données à caractère personnel, à la vie privée, aux droits ou aux intérêts légitimes des personnes concernées. La proposition de règlement prévoit certaines exceptions à cette obligation de notification, notamment lorsque l'autorité nationale est d'avis que le responsable du traitement avait implémenté des mesures techniques appropriées pour les données en question.

De plus, la proposition de règlement prévoit que le responsable du traitement effectuant des activités de traitement représentant un risque particulier doit réaliser une analyse d'impact sur la protection des données à caractère personnel. Plusieurs exemples de traitements présentant des risques particuliers peuvent être donnés: le traitement de données de plus de 5.000 personnes concernées sur une période de 12 mois, ou le traitement de données d'employés dans des systèmes d'archivage de grande ampleur.

L'analyse d'impact tient compte de l'ensemble du cycle de traitement. Dès lors, les violations potentielles de données doivent être documentées et doivent notamment contenir une analyse d'impact sur les droits et libertés des personnes concernées, ainsi qu'une liste des garanties, mesures de sécurité et mécanismes destinés à assurer la protection des données. Les responsables du traitement doivent en outre effectuer des contrôles de conformité périodiques afin de s'assurer que les activités de traitement satisfont aux assurances données dans l'analyse d'impact.

Si l'analyse d'impact indique que les activités de traitement impliquent un haut de degré de risques particuliers pour les droits et libertés des personnes concernées, par exemple suite à l'utilisation de nouvelles technologies spécifiques, le délégué à la protection des données du responsable du traitement, ainsi que l'autorité pour la protection des données chargée de la supervision de ce dernier, doivent être consultées avant de débuter lesdites activités de traitement.

La proposition de règlement prévoit également que toutes les autorités nationales pour la protection des données auront le pouvoir d'imposer des amendes. Ainsi, en cas de non-respect de l'obligation de notification d'une violation de données, une amende pouvant aller jusqu'à 100.000.000 euros ou 5% du chiffre d'affaires mondial pourra être infligée.

Le conseil de l'UE n'a pas encore pris une position finale sur l'ensemble du texte. Néanmoins, en décembre 2013, une version amendée de celui-ci contenant des modifications concernant notamment l'exigence de notification a été rendue publique.

b) La directive sur la sécurité des réseaux et de l'information

La bien moins controversée proposition de directive concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et de l'information dans l'Union (COM (2013) 48) prévoit également des obligations en matière de notification des violations de données. Venant d'être approuvée par le Parlement européen, elle prévoit que tous les exploitants d'infrastructures critiques (énergie, transports, banques, bourse, santé, etc.) doivent notifier l'autorité nationale de tout incident ayant un impact sur la continuité du service.

Un tel impact peut par exemple consister en une violation de données ou un vol de données. À l'heure actuelle, le conseil ne s'est pas encore prononcé sur cette proposition, mais prévoit de le faire bientôt.

Conclusion

Au regard des sanctions – présentes et futures – que la CNPD peut infliger, il est clair que les responsables du traitement de données à caractère personnel doivent savoir comment gérer de manière efficace les violations de données.

Au vu des changements imminents dans toute l'UE visant à rendre obligatoires les notifications de violation de données, il est conseillé aux responsables du traitement de:

1. Procéder à une analyse d'impact: même si une telle analyse n'est pas (encore) formellement obligatoire, il s'agit d'une façon d'analyser si les mesures de sécurité mises en place sont suffisantes.
2. Planifier d'avance la manière de gérer une violation de données
3. Informer la CNPD de la violation: même s'il n'existe pas (encore) d'obligation de notifier une violation de données, le fait de notifier la CNPD (de manière informelle) peut aider le responsable du traitement à déterminer les effets potentiels de la violation de données, en ce compris les besoins de notifier les personnes concernées.

Vincent WELLENS (cf. portrait)
Avocat à la Cour
Partner chez NautaDutilh Avocats Luxembourg
vincent.wellens@nautadutilh.com

Mathilde STENERSEN
Associate chez NautaDutilh Avocats Luxembourg
mathilde.stenersen@nautadutilh.com

www.nautadutilh.com

Le secteur de l'ICT fleurit au Luxembourg : Trois nouvelles entreprises se lancent

Trois sociétés actives dans le secteur des technologies de l'information et de la communication (ICT) ont annoncé le lancement de leurs activités au Luxembourg. Il s'agit de la société japonaise Chatwork qui y établit une filiale, de l'entreprise sud-coréenne SK Broadband et de la création de la firme MTX Connect. Le ministre des Communications et des Médias, Xavier Bettel, a salué l'arrivée de ces entreprises au Luxembourg.

"L'annonce de Chatwork, MTX Connect et SK Broadband de s'établir au Luxembourg montre que les atouts du Luxembourg en tant que plateforme ICT sont désormais connus et reconnus au niveau mondial. En construisant sur ces atouts, la nouvelle stratégie nationale 'Digital Lëtzebuerg' vise à consolider et à développer notre pays comme centre d'excellence pour le développement de services innovants liés aux technologies des communications."

Le Luxembourg, un des sites de prédilection pour les entreprises du secteur ICT

Le ministre de l'Économie, Étienne Schneider, s'est réjoui que les efforts du gouvernement portent leurs fruits que ce soient les investissements importants pour doter le secteur ICT des meilleures infrastructures possibles, les efforts de promotion lors des missions économiques ou l'amélioration du cadre général pour ce type d'entreprise: "Il n'y a pas un argument unique qui a convaincu ces trois entreprises de travailler à partir du Luxembourg, mais il s'agit d'un faisceau d'arguments qui a fait pencher la balance en faveur du Grand-Duché. Le Luxembourg figure aujourd'hui parmi les sites de prédilection pour les entreprises du secteur ICT et nous sommes très fiers d'accueillir ces trois nouvelles sociétés."

Chatwork, une entreprise japonaise, va ouvrir son quartier général européen au Luxembourg afin d'entrer sur l'ensemble du marché de l'UE. Chatwork offre une plateforme de communication pour les entreprises utilisée par 46.000 entreprises dans 170 pays. MTX Connect, une nouvelle société luxembourgeoise, est un fournisseur Internet mobile. Elle a lancé un service de carte pré-payée notamment pour les voyageurs qui peut être utilisé d'ores et déjà au Luxembourg et dans douze autres pays européens.

SK Broadband, un fournisseur d'Internet à ultra haut débit de Corée du Sud, a établi son réseau européen de distribution de contenu au Luxembourg.

Source: ministère de l'Économie