Publié le 1 juin 2011

Soulier Bunch, Cabinet d'avocats d'affaires basé à Paris et Lyon

Lire cet article en ligne

Failles de sécurité : une nouvelle obligation de déclaration bientôt à la charge des entreprises

C'est dans le contexte des piratages récents de Sony que le gouvernement a rendu public son projet d'ordonnance créant une obligation de notification des failles de sécurité (désignant les pertes de données à caractère personnel) à la charge des entreprises responsables de ces données[1].

Les 18 et 19 avril dernier, SONY a été victime d'un piratage massif, provoquant le vol de données à caractère personnel de 77 millions d'utilisateurs du Playstation network[2] (dont 2,2 millions de numéros de cartes de crédit). Elle a ensuite découvert qu'un autre de ses systèmes (Sony Online Entertainment[3]) avait été piraté les 16 et 17 avril, exposant 25 millions de comptes utilisateurs. Alors que l'on considérait que SONY avait désormais la situation sous contrôle, So-Net (autre filiale de SONY) a fait l'objet d'un piratage le 21 mai. Il est aujourd'hui impossible de connaître les répercussions que pourra avoir le vol de ces données à caractère personnel.

Ce qui est certain, c'est que ces failles de sécurité représenteront un coût important pour l'entreprise. Il varie en réalité selon les circonstances, à savoir notamment si les données sont relatives aux cartes bancaires, si une class action est ouverte (ce qui est le cas aux USA et au Canada, où une première action a d'ores et déjà été introduite à l'encontre de SONY. En France, la class action n'existe toujours pas), ou si les autorités compétentes ont le pouvoir d'infliger des amendes (ce qui est le cas en France pour la Commission nationale de l'informatique et des libertés, ci-après « CNIL »).

Ce piratage historique souligne en France la nécessité d'un renforcement des règles existantes.

En matière de failles de sécurité, nombre de pays parmi lesquels figurent les Etats-Unis, l'Allemagne, le Royaume-Uni, et l'Autriche ont choisi la transparence et obligent les entreprises à déclarer leurs pertes de données (« data breach notification »). En France, pour le moment il n'existe pas de telle obligation. En effet, l'article 34 de la loi actuelle Informatique et Liberté impose simplement au responsable du traitement de données à caractère personnel l'obligation de prendre « *toutes précautions utiles pour préserver la sécurité des données*« .

Cependant, l'échéance du délai de transposition du paquet télécom (ensemble de directives européennes régulant le secteur des télécommunications adoptées au niveau européen en 2009 et intégrant des dispositions concernant la notification des failles de sécurité) explique que le gouvernement ait présenté le 3 mai un projet d'ordonnance contenant une telle obligation. L'article 38 de ce projet prévoit que tout fournisseur de services de communications électroniques qui se fait pirater les données à caractère personnel qu'il détient devra en informer la CNIL, voire ses clients.

Il ne sera cependant pas obligatoire d'informer ces derniers dans tous les cas. C'est en effet à la CNIL de décider que, puisque des mesures de sécurité ont été prises, l'entreprise n'est pas obligée de le rendre public : « *si la Commission nationale de l'informatique et des libertés a validé les mesures de protection technologiques mises en œuvre par le fournisseur pour remédier à la violation des données à caractère personnel et constaté que ces mesures ont été appliquées aux données concernées par ladite violation* », ce fournisseur n'est pas dans l'obligation de notifier la faille au principal intéressé.

L'adoption d'une telle règle marquera à coup sûr un réel progrès en matière de sécurité des données à caractère personnel en obligeant les entreprises à faire preuve de transparence vis à vis des autorités et éventuellement des personnes concernées.

Ce piratage historique souligne en France la nécessité d'un renforcement des règles existantes.

En matière de failles de sécurité, nombre de pays parmi lesquels figurent les Etats-Unis, l'Allemagne, le Royaume-Uni, et l'Autriche ont choisi la transparence et obligent les entreprises à déclarer leurs pertes de données (« data breach notification »). En France, pour le moment il n'existe pas de telle obligation. En effet, l'article 34 de la loi actuelle Informatique et Liberté impose simplement au responsable du traitement de données à caractère personnel l'obligation de prendre « *toutes précautions utiles pour préserver la sécurité des données*« .

Cependant, l'échéance du délai de transposition du paquet télécom (ensemble de directives européennes régulant le secteur des télécommunications adoptées au niveau européen en 2009 et intégrant des dispositions concernant la notification des failles de sécurité) explique que le gouvernement ait présenté le 3 mai un projet d'ordonnance contenant une telle obligation. L'article 38 de ce projet prévoit que tout fournisseur de services de communications électroniques qui se fait pirater les données à caractère personnel qu'il détient devra en informer la CNIL, voire ses clients.

Cependant, le projet limite l'obligation de notification aux seuls fournisseurs de services de communications électroniques et ne l'étend pas à l'ensemble des responsables de traitement quelles que soient les données traitées.

A l'heure actuelle, et même si les entreprises n'ont pas l'obligation de rendre publiques les failles de sécurité dont sont victimes leurs systèmes informatiques, il est néanmoins possible d'obtenir des sanctions à l'encontre de l'entreprise qui a perdu des données à caractère personnel.

Une faille de sécurité constitue en effet une violation de la loi Informatique et Liberté. Sur le plan pénal, la loi punit actuellement 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 précité de cinq ans d'emprisonnement et de 300 000 Euros d'amende (Art. 226-17 du Code pénal). Elle punit aussi la divulgation d'information commise par imprudence ou négligence de 3 ans d'emprisonnement et de 100 000 euros d'amende (Art. 226-22 du Code pénal). Si l'obligation de notification prévue par le projet d'ordonnance devait entrer en vigueur, la sanction en cas de manquement de l'entreprise à son obligation de notification serait celle de l'article 226-17 du Code pénal, à savoir 5 ans d'emprisonnement et 300 000 euros d'amende (Article 39 du projet d'ordonnance).

Bien sûr, en l'absence d'obligation de notification, l'existence de sanctions dépend de la connaissance des failles de sécurité. Celles-ci peuvent être portées à la connaissance de la CNIL sur la base d'une plainte ou à l'occasion des enquêtes diligentées à sa propre initiative. C'est précisément ce qu'elle envisage de mettre en œuvre à l'encontre de SONY. Cette enquête lui permettra de savoir combien de personnes sont concernées en France, quelle est la nature des données, quelle a été la faille exacte de sécurité, si les données étaient suffisamment chiffrées, quelles informations ont été envoyées aux personnes victimes. Cette enquête pourrait déboucher sur des sanctions administratives. Les sanctions que peut infliger la CNIL vont du simple avertissement à des sanctions financières pouvant atteindre jusqu'à 150 000 euros.

Il ne sera cependant pas obligatoire d'informer ces derniers dans tous les cas. C'est en effet à la CNIL de décider que, puisque des mesures de sécurité ont été prises, l'entreprise n'est pas obligée de le rendre public : « *si la Commission nationale de l'informatique et des libertés a validé les mesures de protection technologiques mises en œuvre par le fournisseur pour remédier à la violation des données à caractère personnel et constaté que ces mesures ont été appliquées aux données concernées par ladite violation* », ce fournisseur n'est pas dans l'obligation de notifier la faille au principal intéressé.

L'adoption d'une telle règle marquera à coup sûr un réel progrès en matière de sécurité des données à caractère personnel en obligeant les entreprises à faire preuve de transparence vis à vis des autorités et éventuellement des personnes concernées.

---

[1] Consultation publique sur le projet d'ordonnance portant transposition du paquet télécom :

http://www.telecom.gouv.fr/fonds_documentaire/consultations/11/110503projetordonnance.pdf

[2] Ce réseau permet aux utilisateurs de la console PlayStation 3 de Sony de s'affronter en ligne. Il permet aussi d'acheter des jeux, des films ou de la musique en ligne.

[3] Ce service permet notamment de jouer en ligne à Everquest, Champions of Norrath, PlanetSide (Jeux massivement multi-joueurs).