INFORMATIQUE

3 QUESTIONS
Failles de sécurité : quel régime juridique ?

Chloé Torres, avocat, directeur du département Informatique et libertés, ALAIN BENSOUSSAN AVOCATS

1 Que recouvre l'expression « faille de sécurité » ?

L'expression « failles de sécurité » est régulièrement utilisée par les médias qui se font l'écho de comptes clients dérobés lors d'attaques informatiques ou dévoilées sur Internet en raison d'une mauvaise configuration d'un site web. Cette expression recouvre tous les éléments qui portent atteinte à un système de traitement automatisé de données : les erreurs, les bugs mais aussi les fraudes internes et externes. Elle traduit le fait qu'à un instant des données à caractère personnel se trouvent avoir été corrompues. L'article 34 *bis* de la loi *Informatique et libertés* utilise la terminologie de « *violation de données personnelles* » définit de manière extrêmement large comme toute destruction, perte, altération, divulgation ou accès non autorisé à des données.

Entrent dans le champ d'application de la notion de faille de sécurité :
- les failles accidentelles qui proviennent d'une faute, d'une erreur ou d'une négligence ;
- les failles résultant de défaut des progiciels inconnus du responsable de traitement ou de son sous-traitant ;
- les failles ouvertes au moyen de procédés illicites.

La notion de faille est ainsi une caractéristique technique sans lien avec :
- une faute des responsables de traitements ou de leurs sous-traitants ;
- la connaissance effective ou potentielle de la faille ;
- la gravité de la faille.

2 Quelles sont les obligations légales et en quoi consiste votre intervention ?

L'entreprise victime d'une faille de sécurité met en place une cellule de crise habituellement composée de la Direction des systèmes d'information (DSI), du responsable de la sécurité des systèmes d'information (RSSI), de la direction juridique et d'un avocat spécialisé. Cette cellule de crise est chargée de piloter les six principales actons suivante ;
- action 1 : identifier par le biais d'un audit de sécurité la faille et la corriger ;
- action 2 : constituer le dossier de preuve technique en concertation avec la DSI ;
- action 3 : qualifier juridiquement l'infraction (atteinte à un système de traitement automatisé de données, vol d'information, tentative de chantage…) puis déposer plainte auprès du procureur de la République afin qu'il diligente une enquête préliminaire. Parallèlement au dépôt de plainte, nous prenons attache avec la brigade d'enquêtes sur les fraudes aux technologies de l'information (BEFTI), afin de suivre l'évolution des investigations menées par les services de police et en orienter l'exercice ;
- action 4 : déterminer la stratégie de communication vis-à-vis de la CNIL. L'article 34 *bis* de la loi *Informatique et libertés* impose au responsable de traitement de notifier certaines failles de sécurité à la CNIL, et ce sans délai. Cette obligation de

Suite page 6

En mouvement

Philippe Laye rejoint le cabinet ***PDGB*** au 1er janvier 2015. Exerçant précédemment chez Frêche & Associés, il est accompagné de son collaborateur ***Théophile Faure-Cachard.***

Ayant une activité en droit des affaires, tant en conseil qu'en contentieux, Philippe Laye intervient depuis plus de vingt ans auprès d'une clientèle française et internationale composée de PME et de grands groupes, dans les divers secteurs de l'économie et notamment dans ceux de la distribution, les nouvelles technologies, l'industrie et le courtage d'assurance.

Il devient le 4e associé du département Droit commercial-Contentieux-Arbitrage de PDGB, avec les associés Xavier Hugon, Bertrand Jardel et Philippe Julien.

Le cabinet d'avocats ***Bignon Lebray*** poursuit sa croissance et renforce son positionnement en Private Equity et en Fusions-Acquisitions avec la cooptation de ***Edouard Waels*** en qualité d'associé, à compter du 1er janvier 2015. Fort d'une expérience d'une dizaine d'années en conseil sur des opérations Smid Cap en M & A et en capital investissement (capital risque, capital développement et LBO), Edouard intervient tant dans l'univers des start-ups que pour des entreprises plus matures (PME-ETI), cotées ou non.

Il assiste dans cette perspective une clientèle française et internationale, principalement des investisseurs financiers (fonds d'investissement, *family office* et *business angels*), des groupes de sociétés, des actionnaires privés et des dirigeants d'entreprise, dans le cadre de la structuration et la réalisation de leurs opérations de haut de bilan, de croissance externe ou d'investissement.

Lamy & Associes développe son département Concurrence, Distribution, Contrats commerciaux : ***Luc-Marie Augagneur*** (37 ans), avocat au barreau de Lyon depuis 2003, après 4 ans (2003-2007) au sein de Lamy & Associés avait intégré le cabinet Jakubowicz, Mallet-Guy & Associés en qualité d'associé

notification des failles de sécurité ne s'applique qu'aux failles correspondant :
- à des traitements de données à caractère personnel,
- mis en œuvre dans le cadre de la fourniture au public de services de communications électroniques, c'est-à-dire les traitements mis en œuvre par les fournisseurs d'accès à internet,
- y compris ceux prenant en charge les dispositifs de collecte de données et d'identification,
- opérés aux moyens de réseaux de communications électroniques ouverts au public.

Tous les autres types de faille de sécurité portant sur des traitements de données à caractère personnel ne sont pas soumis à l'obligation de notification à la Cnil. Il peut toutefois parfois être judicieux d'informer la Cnil de la situation. Il peut, également être opportun, dans certains cas, d'informer les personnes concernés voir les partenaires ;
- action 5 : gestion de la communication auprès des médias ;
- action 6 : assurance. La ligne assurantielle n'est pas à négliger puisque l'entreprise doit déclarer le sinistre auprès de la compagnie d'assurance.

3 Quelles sont les tendances ?

La proposition de règlement européen sur la protection des données qui devrait être adopté fin 2015 début 2016 vise à étendre à l'ensemble des entreprises l'obligation de notifier auprès de la CNIL toute violation de données à caractère personnel. Le règlement précise les éléments devant obligatoirement figurer sur la notification effectuée auprès de l'autorité de contrôle, dans les 24 heures de la constatation de la violation de sécurité. De même, le responsable du traitement devra conserver une trace documentaire des violations de données à caractère personnel. Il devra également informer les personnes concernées dès lors que la violation est susceptible de porter atteinte à la protection des données à caractère personnel ou à la vie privée de la personne concernée. Cette communication devra être effectuée après avoir réalisé la notification auprès de l'autorité de contrôle et devra décrire notamment la nature de la violation ainsi que les mesures à prendre pour atténuer les conséquences négatives.

Focus

Financement de l'aide juridictionnelle

Aux fins d'améliorer le financement de l'aide juridictionnelle, la loi de finances comporte les mesures d'ordre fiscal suivantes :
- augmentation de 2,6% du taux d'impositions des contrats d'assurance de protection juridique : taux spécifiques de 11,6% au lieu du taux par défaut de 9%. - Ce dernier taux de 9% reste cependant applicable aux assurances ayant pour objet exclusif ou principal la prise en charge de la défense pénale ou le recours en réparation d'un préjudice personnel suite à un accident. Cette source de financement devrait rapporter 25 millions d'euros par an sur les trois ans à venir ;
- augmentation de la taxe forfaitaire sur la taxe des huissiers de justice de 9,15 € à 11,16 € ce qui générera 11 millions d'euros par an ;
- augmentation du droit fixe de procédure devant les juridictions répressives :
  - 31 € au lieu de 22 € pour les ordonnances pénales, contraventionnelles ou correctionnelles, pour les autres décisions des tribunaux de police et pour les décisions ne portant pas sur le fond ;
  - 127 € au lieu de 90 € pour les décisions des tribunaux correctionnels (254 € au lieu de 180 € en cas de non-comparution personnelle) ;
  - 169 € au lieu de 120 € pour les décisions de la chambre des appels correctionnels ;
  - 527 € au lieu de 375 € pour les décisions de cours d'assises ;
  - 211 € au lieu de 150 € pour les décisions de la Cour de cassation.

Ces mesures ont pris effet au 1er janvier 2015 *(CNB, 15 janv. 2015)*.

ENTRÉES EN VIGUEUR

DATE	RÉFÉRENCES	OBSERVATIONS
1er janv. 2015	**D. n° 2014-506, 19 mai 2014 modifiant l'article R. 743-140 du code de commerce relatif au tarif général des greffiers des tribunaux de commerce**	Le texte entre en vigueur le 1er janvier 2015 pour les dispositions de l'article 1er et le 1er juillet 2014 pour les dispositions de l'article 2.
1er janv. 2015	**D. n° 2012-120, 30 janv. 2012 pris pour l'application de la loi n° 2011-850 du 20 juillet 2011 de libéralisation des ventes volontaires de meubles aux enchères publiques**	Ce texte concerne les courtiers de marchandises assermentés, les opérateurs de ventes volontaires de meubles aux enchères publiques.
1er janv. 2015	**D. n° 2011-873, 25 juill. 2011 relatif aux installations dédiées à la recharge des véhicules électriques ou hybrides rechargeables dans les bâtiments et aux infrastructures pour le stationnement sécurisé des vélos**	Les dispositions du décret s'appliquent : - aux bâtiments neufs dont la date de dépôt de la demande de permis de construire est postérieure au 1er janvier 2012 ; - aux bâtiments existants à compter du 1er janvier 2015.