SYLVAIN MÉTILLE

ANNONCER LES FAILLES DE SÉCURITÉ N'EST PLUS UNE OPTION

Nouvelles obligations lorsque des données personnelles sont exposées [1]

Le Règlement général de protection des données et la Loi sur la protection des données révisée prévoient des obligations d'annoncer dans des délais extrêmement courts les violations de la sécurité des données. Ces obligations ne peuvent être remplies que si l'entreprise s'y est préalablement préparée.

1. INTRODUCTION

Lorsque l'on parle de failles de sécurité, on pense surtout à *Equifax* [2], *Adobe* [3], *TalkTalk* [4], *Sony* [5], *Target* [6], etc., soit pour l'essentiel des sociétés américaines. Mais cela existe également en Suisse, sauf qu'on le sait moins. Hormis peut-être le vol de données d'*Hervé Falciani* chez *HSBC Private Bank à Genève* en 2007 ou la tentative avortée d'un informaticien du service de renseignement de la Confédération en 2012. On a pourtant pu lire dans la presse en 2013 que la *Banque Coop* a envoyé 41 000 relevés de comptes à de mauvais destinataires à cause d'une erreur de programmation informatique et que la *NZZ* a reçu cinq bandes de sauvegarde contenant des données confidentielles de *Swisscom*. Ou encore en 2014, lorsque des factures de clients de *UPC Cablecom* sont accessibles sur le site web de l'opérateur. Fin août 2017, la Centrale d'enregistrement et d'analyse pour la sûreté de l'information *MELANI* annonçait avoir reçu environ 21 000 combinaisons de noms d'utilisateur et mots de passe [7]. On pourrait aussi mentionner tous les courriels mal adressés, les ordinateurs, clés *USB* et autres supports de données perdus ou volés dont le grand public n'a jamais connaissance, ainsi que les actes d'employés indélicats.

Cela pourrait pourtant bien changer, et rapidement. Dès mai 2018 en Europe et peu après en Suisse, des obligations d'annonce seront introduites lorsque des données personnelles sont exposées à l'image de ce qui existe déjà dans 48 Etats américains [8]. C'est en effet en Californie qu'a été adoptée la première loi du genre en 2002 [9].

SYLVAIN MÉTILLE,
DR EN DROIT, AVOCAT,
CHARGÉ DE COURS,
UNIVERSITÉ DE LAUSANNE,
LAUSANNE/VD,
METILLE@HDCLEGAL.CH

L'Union européenne (UE) s'est également dotée d'une directive sur les infrastructures critiques, la Directive NIS [10]. Elle s'applique aux opérateurs de services essentiels soit les entités qui fournissent des services essentiels au maintien des activités sociales ou économiques, qui sont tributaires des réseaux et systèmes d'information et dont un incident aurait un effet disruptif important sur la fourniture du service ainsi qu'aux fournisseurs de services numériques [11]. Le but de cette directive est notamment de mettre en place un mécanisme permettant de protéger les informations sensibles qui pourraient, en cas de divulgation, être utilisées pour planifier ou mettre en œuvre des actions visant à provoquer l'arrêt ou la destruction d'installations d'infrastructures critiques.

Même hors des infrastructures critiques, si une faille a eu lieu et que des données personnelles sont impliquées, elle peut causer aux personnes concernées des dommages physiques, matériels ou un préjudice moral tels qu'une perte de contrôle sur leurs données, une discrimination, une usurpation d'identité, une perte financière, une atteinte à la réputation, etc. Il est donc primordial de réagir vite. L'entreprise devra prendre toutes les mesures utiles pour limiter les dégâts, sauver son image et, c'est la nouveauté, informer rapidement l'autorité compétente et dans certains cas les personnes concernées.

Les entreprises doivent évidemment anticiper ce changement, car lorsque la faille survient le temps manquera pour mettre en place un processus efficace. Pire encore, le devoir d'annonce pourrait être tout simplement oublié, malgré les risques de sanctions supplémentaires. Il est donc nécessaire de bien comprendre ce qu'est une faille de sécurité (2), ce qu'impose la loi (3) et comment s'y préparer (4).

2. UNE FAILLE DE SÉCURITÉ

2.1 Un peu de terminologie. On parle tantôt de faille de sécurité en référence à la terminologie anglophone de *security breach* ou *data breach,* tantôt de violations de la sécurité des données ou de violations de données à caractère personnel. Le projet de nouvelle *loi fédérale sur la protection des données*

(nPD) [12] parle désormais de violation de la sécurité des données et le *Règlement européen général sur la protection des données (RGPD)* de violation de données à caractère personnel. Nous préférons parler de faille de sécurité (ce qui peut inclure ou non des données personnelles selon la définition retenue). L'avant-projet de révision de la LPD utilisait la notion de violation de la protection des données (et non pas de la sécurité des données), ce qui pouvait laisser penser aussi à une violation volontaire des principes ou de la loi par le responsable du traitement. Une telle violation intentionnelle n'est pas une faille de sécurité, contrairement à une violation accidentelle ou le fait d'un tiers ou d'un employé contrairement à ce que le responsable du traitement a prévu. Le projet de nLPD définit maintenant à l'art. 4 let. g une violation de la sécurité des données comme toute violation de la sécurité, sans égard au fait qu'elle soit intentionnelle ou illicite, entraînant la perte de données personnelles, leur modification, leur effacement ou leur destruction, leur divulgation ou un accès non autorisé à ces données.

Dans l'établissement de bonnes pratiques, il est aussi important d'inclure toutes les failles de sécurité, qu'elles concernent ou non des données personnelles [13].

Le RGPD a aussi une vocation d'application extraterritoriale, en particulier aux responsables de traitement établis hors de l'UE mais qui offrent des biens ou des services à des personnes établies dans l'UE, ou font un suivi du comportement de ces personnes (profilage) au sein de l'UE [14]. Une société suisse qui perd des données de citoyens suisses et européens, même si elle est établie exclusivement en Suisse, pourrait devoir gérer les conséquences au regard des droits suisse et européen.

2.2 La faille. Une faille de sécurité est une mise en danger abstraite ou potentielle des données. L'art. 4 ch. 12 RGPD définit une violation de données à caractère personnel comme une violation de la sécurité entraînant, de manière accidentelle ou illicite, la destruction, la perte, l'altération, la divulgation non autorisée de données à caractère personnel transmises, conservées ou traitées d'une autre manière, ou l'accès non autorisé à de telles données.

Il n'est pas nécessaire qu'un résultat ou un dommage se soit produit. On sera d'ailleurs très souvent dans l'incapacité de le démontrer ou même de le savoir. On considère par exemple qu'il y a une faille dès que la sécurité des données n'est plus garantie et que les données ont été exposées, c'est-à-dire qu'il y a potentiellement eu un accès aux données ou un traitement non autorisé. Il peut s'agir d'une perte de contrôle (publication des données, oubli d'un support de données dans un lieu accessible, défaillance de mesures de protection ou de contrôle d'accès, etc.), de l'obtention des données par une personne non autorisée (hacking, copie, vol, etc.), de l'utilisation abusive des données par un tiers voire d'un effacement non autorisé (mise hors d'usage accidentelle, chiffrement par rançongiciel, etc.).

L'acte est le plus souvent causé par un tiers, mais parfois aussi par un collaborateur qui outrepasse ses compétences. Une organisation ou une infrastructure informatique défaillante [15] augmente sensiblement le risque de failles.

2.3 Les données. Les données concernées sont principalement des données personnelles. La LPD et le RGPD ont pour but de protéger la personnalité et les droits fondamentaux des personnes en lien avec le traitement de données les concernant. Elles visent les données personnelles, soit toutes les données qui se rapportent à une personne identifiée ou identifiable [16]. La notion est vaste et inclut notamment un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, une adresse IP, un numéro de compte, etc. Celui qui décide du but et des moyens utilisés pour traiter les données est appelé responsable du traitement.

L'on relèvera que ni le projet de nLPD, ni le RGPD ne prévoient qu'un nombre minimum de personnes doivent être concernées par la faille de sécurité. Il suffit à cet égard que les données d'une seule personne soient potentiellement affectées par la faille de sécurité pour que le responsable du traitement doive procéder à l'annonce.

La Directive NIS (Network Security and Information) impose aux opérateurs de services essentiels qu'ils notifient à l'autorité compétente, sans retard injustifié, les incidents qui ont un impact sur la continuité des services essentiels qu'ils fournissent [17]. Le type de données concernées (personnelles ou non) ne joue ici aucun rôle.

Des données, personnelles ou non, peuvent finalement être soumises à des obligations spécifiques par un contrat, notamment dans le cadre d'accords de confidentialité. C'est courant s'agissant de données commerciales confidentielles ou stratégiques. Dans ce cas, le contrat prévoit des obligations qui seront le plus souvent une obligation d'informer le co-contractant et parfois une sanction.

3. DES OBLIGATIONS D'ANNONCE

3.1 Les destinataires de l'annonce

3.1.1 L'annonce à l'autorité. L'art. 22 al. 1 nLPD prévoit que le responsable du traitement notifie sans délai au *Préposé fédéral à la protection des données et à la transparence suisse (PFPDT)* tout traitement non autorisé ou toute perte de données personnelles. L'art. 33 RGPD prévoit une obligation similaire. Dans le cas d'un responsable du traitement établi en Suisse mais soumis au RGPD [18], l'annonce exigée par le RGPD devrait être faite non pas au PFPDT mais à l'autorité de contrôle compétente de chaque Etat membre où des personnes sont concernées par la faille [19].

Ce n'est que si la violation ne présente vraisemblablement pas de risques pour la personnalité et les droits fondamentaux des personnes concernées que le responsable du traitement peut y renoncer. Cette exception vise à éviter la notification de violations insignifiantes, mais son interprétation doit rester restrictive. C'est au responsable du traitement qu'il revient d'évaluer les conséquences possibles de la faille pour les personnes concernées et de décider s'il est hautement improbable que le traitement non autorisé présente un risque et donc s'il peut renoncer à informer le PFPDT, respectivement les autorités européennes concernées.

Certaines législations ne prévoient pas d'annonce à une autorité de protection des données, mais à une autorité pénale. C'est par exemple le cas en Californie où la personne ou l'entreprise privée qui y exploite une activité commerciale

doit annoncer au Procureur général toute faille de sécurité qui touche les données personnelles de plus de 500 résidents californiens.

3.1.2 L'annonce aux personnes concernées. Dans certains cas, une annonce à l'autorité ne suffit pas et il faut en plus informer les personnes concernées. L'art. 22 al. 4 nLPD le prévoit seulement si cela est nécessaire à leur protection ou si le PFPDT l'exige. L'art. 34 al. 1 RGPD prévoit une telle obligation si l'autorité de protection des données l'exige, mais également si la faille est susceptible d'engendrer un risque élevé pour les droits et libertés d'une personne.

Même si le responsable du traitement peut obliger tous les utilisateurs à utiliser un nouveau mot de passe pour son service, il n'a pas de contrôle sur l'utilisation malheureusement trop fréquente d'un même mot de passe pour différents services. En les informant que leur mot de passe a été exposé, il leur permet de prendre les dispositions nécessaires pour se protéger par exemple en modifiant ce même mot de passe auprès de tiers, ce sur quoi le responsable du traitement ne peut évidemment pas agir directement.

Une communication plus limitée aux personnes concernées qu'à l'autorité compétente se justifie pour éviter une certaine fatigue ou désensibilisation. À force de recevoir des notifications pour des cas insignifiants, les personnes concernées risqueraient de ne plus réagir en cas de faille sérieuse.

3.1.3 L'annonce publique. La nLPD ne prévoit pas d'annonce publique comme c'est pourtant le cas dans plusieurs États américains. Le RGPD prévoit en revanche une communication publique dans le cas où la communication aux personnes concernées exigerait des efforts disproportionnés. Une communication large, par exemple à tous les clients, qu'ils soient victimes ou non, devrait aussi être admise.

L'annonce publique ne dispense en principe pas le responsable du traitement de communiquer, dans toute la mesure du possible, la faille individuellement aux personnes concernées.

3.2 Les modalités d'annonce

3.2.1 Le principe. C'est au responsable du traitement qu'il revient seul de décider s'il doit ou non annoncer la faille. Si la faille survient chez un sous-traitant, celui-ci a une obligation légale d'en informer le responsable du traitement. Ce dernier doit ensuite apprécier les risques et décider si la violation doit être notifiée au PFPDT et éventuellement à la personne concernée.

Sauf obligation imposée par l'autorité, c'est aussi le responsable du traitement qui doit déterminer si l'information des personnes concernées est nécessaire. Le responsable du traitement peut évidemment se faire conseiller dans ses choix par un tiers. À cet égard il est recommandé d'inclure rapidement un avocat externe dans la discussion, ce qui permet d'invoquer le secret de l'avocat et de ne pas avoir à fournir à l'autorité les documents liés aux discussions entourant par exemple le choix de ne pas annoncer la faille. Les personnes présentes seront ainsi libres de parler de la faille sans devoir la minimiser et sans que l'on puisse ensuite retenir ou leur reprocher d'avoir envisagé certains faits.

Le responsable du traitement doit donc déterminer s'il y a une faille (et donc une obligation d'annonce) ou non. Dans le premier cas, il sera toutefois tenté d'évaluer les conséquences de l'annonce. En effet, si l'omission d'annoncer peut être sanctionnée notamment en Europe, le fait d'annoncer ne garantit pas une immunité (en particulier sous l'angle civil) en lien avec des manquements précédant la faille et qui seraient alors révélés.

Le PFPDT n'a pas de pouvoir de sanction et est soumis au secret de fonction. Même s'il sera supposé d'énoncer certains manquements au ministère public, on peut s'attendre à ce qu'il concentre plutôt ses efforts pour amener le responsable du traitement à corriger les erreurs constatées suite à l'annonce, plutôt que de renoncer à l'annonce dans le but d'éviter une sanction certaine pour violation des principes de la LPD (et seulement risquer une sanction potentielle du même ordre pour ne pas avoir annoncé). Contrairement à l'avant-projet, le projet de nLPD prévoit maintenant qu'une annonce de faille de sécurité ne peut être utilisée dans le cadre d'une procédure pénale contre la personne tenue d'annoncer qu'avec son consentement (art. 22 al. 6 nLPD).

3.2.2 Les exceptions. Même lorsque les conditions obligeant l'annonce sont réunies, le projet de nLPD prévoit que le responsable du traitement peut, dans des cas particuliers, restreindre la notification à la personne concernée, la différer ou y renoncer. Il s'agit par exemple de cas où une loi au sens formel le prévoit, les intérêts prépondérants d'un tiers l'exigent ou encore que les intérêts prépondérants du responsable du traitement l'exigent. Dans ce dernier cas, il faut encore que le responsable du traitement ne communique pas les données personnelles à des tiers [20]. L'information au PFPDT reste due et un intérêt prépondérant ne saurait s'y opposer, étant entendu que le PFPDT est soumis au secret de fonction.

Le RGPD prévoit également des exceptions si des mesures de protection ont été appliquées aux données les rendant incompréhensibles pour toute personne qui n'est pas autorisée à y avoir accès, en particulier si elles sont chiffrées, si des mesures ont été prises pour empêcher le risque élevé de se matérialiser ou si cela exigerait des efforts disproportionnés.

Si les données sont chiffrées et qu'elles ne peuvent pas être déchiffrées, on devrait considérer qu'il ne s'agit pas de données personnelles et que les obligations d'annonce de la LPD et du RGPD ne s'appliquent pas.

3.2.3 Les délais. La nLPD impose une communication «sans délai» au PFPDT, autrement dit dès que le traitement non autorisé est connu. Cela dépendra des circonstances concrètes et notamment des informations disponibles, mais aussi du risque créé pour la personne concernée. Plus le risque est élevé ou le nombre de personnes concernées important, plus la notification devra intervenir rapidement.

L'art. 33 RGPD prévoit une notification à l'autorité nationale de protection des données dans les meilleurs délais et lorsque c'est possible 72 heures au plus tard après en avoir pris connaissance. Si la notification n'a pas lieu dans les 72 heures, elle est accompagnée des motifs du retard.

Il s'agit de délais extrêmement courts, même si le projet initial de RGPD prévoyait seulement 24 heures. Pour pouvoir annoncer la faille, il faut d'abord avoir identifié son objet, son étendue, ses conséquences, les personnes concernées et celles qui sont épargnées, etc. Des informations pourront d'ailleurs être fournies de manière échelonnée à l'autorité, car il est courant de ne pas toutes les avoir à temps et il ne serait pas justifié d'attendre d'avoir l'intégralité des documents à disposition.

Lorsqu'une communication est due aux personnes concernées, elle doit être effectuée aussi rapidement que possible. Il faudra néanmoins tenir compte des circonstances particulières du cas. Parfois la nécessité d'atténuer un risque immédiat de dommage pourrait justifier d'adresser rapidement une communication aux personnes concernées, alors que la nécessité de mettre en œuvre des mesures appropriées empêchant la poursuite de la violation ou la survenance de violations similaires peut justifier un délai plus long dans d'autres cas.

3.2.4 Le contenu. Contrairement à l'avant-projet, le projet de nLPD précise à son art. 22 que l'annonce doit au moins indiquer la nature de la violation de la sécurité des données, ses conséquences et les mesures prises ou envisagées pour remédier à la situation. L'art. 33 RGPD exige au moins la description de la nature de la faille, y compris, si possible, les catégories et le nombre approximatif de personnes concernées par la violation et les catégories et le nombre approximatif d'enregistrements de données à caractère personnel concernés; la mention du nom et les coordonnées du délégué à la protection des données ou d'un autre point de contact auprès duquel des informations supplémentaires peuvent être obtenues; la description des conséquences probables de la faille et les mesures prises ou à prendre pour remédier à la faille, y compris le cas échéant, les mesures pour en atténuer les éventuelles conséquences négatives.

La communication aux personnes concernées devrait, en plus des informations décrites ci-dessus, décrire la nature de la faille et formuler des recommandations à la personne concernée pour atténuer les effets négatifs potentiels.

En Californie, le responsable du traitement doit compléter un formulaire type qui décrit précisément l'origine de la faille de sécurité, les informations qui ont été touchées, les mesures qu'il va prendre pour y remédier ainsi que les mesures que les personnes concernées peuvent prendre. Il doit également mentionner toute autre information importante et donner les coordonnées téléphoniques d'une personne de contact ou d'un site Internet qui permettront aux personnes concernées d'obtenir de plus amples informations.

3.2.5 Les autres obligations. Le RGPD impose en outre une obligation de documenter toute faille en indiquant les faits, les effets et les mesures prises pour y remédier. Cette obligation n'a pas été prévue dans le projet de nLPD mais on peut imaginer qu'elle sera prévue dans l'ordonnance.

3.3 Les sanctions. Le responsable du traitement ou une personne physique en son sein qui intentionnellement n'informe pas le PFPDT ou la personne concernée en cas de faille de sécurité risquait une amende pénale pouvant aller jusqu'à CHF 500 000 selon l'avant-projet [21]. De manière surprenante, il n'y a plus de sanction dans le projet de nLPD. Le PFPDT peut en revanche ordonner à un repsonsable de traitement d'annoncer la faille (art. 45 al. 3 let. 1 nLPD). C'est seulement le non respect de cette décision qui pourrait ouvrir la voie à une sanction pénale, et pour autant encore que le responsable de traitement en ait été préalablement menacé par le PFPDT (art. 57 nLPD).

Au niveau européen, les amendes sont sensiblement plus élevées mais elles visent l'entreprise et non pas une personne physique. Le responsable du traitement et le sous-traitant peuvent se voir infliger une amende administrative pouvant s'élever jusqu'à EUR 10 000 000 ou, dans le cas d'une entreprise, jusqu'à 2% du chiffre d'affaires annuel mondial total de l'exercice précédent, le montant le plus élevé étant retenu [22].

4. QUELQUES RECOMMANDATIONS

Lorsqu'une faille est découverte, il faut agir vite (et bien). Il est donc impératif d'avoir défini préalablement une procédure et que chaque employé connaisse le responsable interne à alerter et les informations à lui transmettre.

Ce responsable devra être formé et avoir identifié toutes les personnes à impliquer potentiellement. Il doit avoir les moyens de les contacter rapidement, y compris les intervenants externes.

De nombreux aspects doivent être pris en compte dans l'élaboration de la procédure et du plan de gestion de crise, en particulier les conséquences légales, l'atteinte à la réputation, le risque d'une attaque, les compétences décisionnelles, etc. Il est aussi important de déterminer quelles données pourraient être concernées et quelles failles sont les plus probables.

Une approche fine et un plan détaillé adapté à chaque entreprise est absolument nécessaire. Le plan devra être suffisamment détaillé pour permettre de trouver en urgence toutes les informations utiles. Voici déjà quelques grandes lignes:

→ *Alerter.* Celui qui découvre la faille doit immédiatement alerter le responsable de la sécurité (ou toute autre personne désignée) et lui donner toutes informations dont il dispose (qui est impliqué, quelles données sont potentiellement concernées, qui est au courant de la faille et s'il y a des mesures immédiates à prendre).

→ *Réunir.* Le responsable doit réunir la direction et les responsables juridique, informatique et communication (éventuellement un avocat externe et un conseiller en relations publiques). Il peut être utile d'intégrer un avocat externe couvert par le secret professionnel afin de ne pas avoir à dévoiler tous les documents en cas de poursuites ultérieures. La répartition des rôles et les responsabilités de chacun doivent être rapidement vérifiées, de même que le mode de fonctionnement de ce groupe et la manière dont les actions sont coordonnées. On s'assurera également d'avoir un moyen de communication fiable entre tous les responsables.

→ *Analyser.* Parallèlement, il faut déterminer quelles données sont concernées, ainsi que les circonstances et l'ampleur de la faille. Sur la base de ces premières informations, chaque res-

ponsable indiquera quelles mesures doivent être prises dans son domaine de responsabilité. Dans la mesure du possible on recherchera déjà la cause de la faille.

→ *Prendre les premières mesures et documenter.* On prendra sans délai les mesures urgentes de protection comme rendre inaccessibles les données qui peuvent encore l'être ou réinitialiser ou bloquer des droits d'accès, les mesures de continuité pour restaurer les données si cela est envisageable et les mesures de conservation pour sauvegarder les preuves et s'assurer qu'elles ne soient pas corrompues.

On gardera une trace de toutes les informations obtenues et les démarches effectuées.

→ *Communiquer.* Sur la base des premières informations disponibles, on décidera si et quand il faut informer le public, les autorités concernées, l'assurance et les employés. Dans le cas où l'entreprise décide de ne pas dévoiler la faille (immédiatement), il faut néanmoins déjà prévoir une réponse à utiliser en cas de besoin. Dans la mesure du possible, il est recommandé de ne pas communiquer la faille dont l'entreprise a été victime avant d'avoir pu en déterminer précisément l'ampleur et les conséquences. Si nécessaire pour respecter les délais, on fera une communication limitée à l'autorité, en expliquant pourquoi il n'est pas possible d'en savoir plus et donc d'en dire plus pour l'instant.

S'il apparaît que la faille est causée par un agissement de nature pénale, l'entreprise devra décider dans quelle mesure et à quel stade elle souhaite impliquer les autorités judiciaires et policières.

Il ne faudra finalement pas oublier les employés, qui devront être rassurés et à qui il faudra donner les informations leurs permettant de défendre l'image de l'entreprise. Il est utile de leur remettre un document avec les explications qu'ils peuvent partager publiquement si des questions leur sont posées.

→ *Gérer.* Une fois l'urgence passée, il convient d'analyser plus en détail la faille, son origine et ses conséquences. On profitera aussi de compléter ou de corriger les annonces effectuées préalablement. On modifiera également tout ce qui peut l'être pour éviter qu'une faille identique ou similaire ne se reproduise. Ensuite, on s'occupera encore de la réputation de l'entreprise, des procédures judiciaires et d'éventuels dédommagements.

→ *Améliorer.* Ce n'est pas parce que la crise est passée qu'il n'y aura plus rien à faire. Au contraire, c'est le moment d'évaluer la manière dont elle a été gérée et d'améliorer les procédures mises en place, ainsi que de s'entraîner à gérer ce genre de situations. ■

Notes: **1)** L'auteur remercie Me Nadja Nguyen Xuan pour sa relecture et son aide dans l'élaboration du texte. **2)** En juillet 2017, Equifax, une des plus grosses entreprises américaines actives dans l'établissement d'attestations de solvabilité, a été victime d'un incident de sécurité lequel a mené à la divulgation de données sensibles de 143 millions de personnes, soit presque la moitié des habitants des Etats-Unis: «Equifax Says Cyberattack May Have Affected 143 Million in the U.S», Tara Siegel Bernard, Tiffany Hsu, Nicole Perlroth et Ron Lieber, in The New York Times, 7 septembre 2017, https://www.nytimes.com/2017/09/07/business/equifax-cyberattack.html?mcubz=3. **3)** En 2013, des hackers sont parvenus à dérober des informations relatives aux comptes des utilisateurs, y compris les numéros de cartes de crédit. Adobe parlait au début de 3 millions de personnes concernées, alors qu'il pourrait y en avoir jusqu'à 150 millions: «Over 150 million breached records from Adobe hack have surfaced online», Chris Welch, in The Verge, 7 novembre 2013, https://www.theverge.com/2013/11/7/5078560/over-150-million-breached-records-from-adobe-hack-surface-online. **4)** En octobre 2015, les données personnelles de 157 000 clients de Talk Talk ont été volées par des hackers. Il s'agissait de leurs informations bancaires, de leur date de naissance ainsi que de leur adresse. Une amende de GBP 400 000 a été imposée par l'autorité anglaise de protection des données. Une nouvelle amende de GBP 100 000 a été imposée en 2017 suite à l'exposition de données relatives à plus de 20 000 personnes: Communiqués de l'ICO des 5 octobre 2016 et 10 août 2017: https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2017/08/personal-data-belonging-to-up-to-21-000-talktalk-customers-could-have-been-used-for-scams-and-fraud/ et https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2016/10/talktalk-gets-record-400-000-fine-for-failing-to-prevent-october-2015-attack/. **5)** En 2014, des hackers sont parvenus à dérober des informations confidentielles de Studio Sony Pictures telles que des informations personnelles des employés de l'entreprise, des courriels, le montant des salaires des employés ainsi que des films qui n'avaient pas encore été rendus publics: «The Sony Pictures hack, explained», Andrea Peterson, in The Washington Post, 18 décembre 2014, https://www.washingtonpost.com/news/the-switch/wp/2014/12/18/the-sony-pictures-hack-explained/?utm_term=.e76a725db3d1. **6)** Fin 2013, Target a été victime d'une cyberattaque qui a permis aux hackers de dérober des données de plus de quarante millions de clients de l'entreprise qui s'étaient rendus dans un magasin de l'enseigne durant la période des fêtes de fin d'année. Grâce à un malware, les hackers ont été en mesure d'accéder aux données personnelles des clients de Target, tels que leur nom, adresse, numéro de téléphone, adresse email ainsi que les détails des cartes de paiement employées: «Massive Target credit card breach new step in security war with hackers: experts», Keith Wagstaff, NBC News, 19 décembre 2013, https://www.nbcnews.com/technology/massive-target-credit-card-breach-new-step-security-war-hackers-2D11778083. **7)** Communiqué de MELANI du 29 août 2017, https://www.melani.admin.ch/melani/fr/home/documentation/lettre-d-information/passwoerter-von-21000-e-mail-konten-im-umlauf.html. **8)** Seuls l'Alabama et le South Dakota n'ont pas de lois sur les failles de sécurité. Le District of Columbia, Guam, Puerto Rico and the Virgin Islands ont aussi adopté des dispositions contraignantes. **9)** California Civil Code §§ 1798.29 et 1798.82. **10)** Directive 2016/1148 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union. **11)** Banques, opérateurs dans le domaine de l'énergie, des transports et dans le secteur de la santé, places de marchés en ligne, moteurs de recherches ou encore services informatiques Cloud. **12)** Le Conseil fédéral a adopté un projet de révision totale de la loi sur la protection des données (nLPD) le 15 septembre 2017. Le texte sera publié officiellement prochainement mais il est déjà disponible en ligne: https://www.ejpd.admin.ch/ejpd/fr/home/aktuell/news/2017/2017-09-150.html. **13)** Si des plans ou documents confidentiels sont concernés, l'entreprise voudra le savoir et s'organiser en conséquence, même si elle ne doit pas informer une autorité en particulier. **14)** Si cela signifie que les autorités européennes de protection des données et les tribunaux pourraient l'appliquer à des entités exclusivement suisses, cela ne signifie pas pour autant qu'une sanction serait reconnue par les autorités suisses et donc exécutable en Suisse. Le risque est en revanche non négligeable si l'entité suisse a une succursale ou des actifs en Europe qui pourraient être saisis. **15)** Logiciels non mis à jour, mots de passe faciles à trouver, droits d'accès mal paramétrés, etc. **16)** Art. 3 let. a LPD et 4 let. a nLPD, art. 4 ch. 1 RGPD. **17)** Art. 14 al. 3 Directive NIS. Une obligation identique s'applique aux fournisseurs de service numérique (art. 16 al. 3 Directive NIS). **18)** Parce qu'il offre par exemple des biens et services à des personnes qui se trouvent sur le territoire de l'UE (art. 3 al. 2 RGPD). **19)** Le responsable du traitement qui n'a pas d'établissement dans l'UE, même s'il a nommé un représentant, ne bénéficie pas du mécanisme de contrôle de la cohérence et de l'autorité de contrôle chef de file: avis WP 244 du G29 «Guidelines for identifying a controller or processor's lead supervisory authority», p. 10. **20)** Les sous-traitants ne sont pas considérés comme des tiers. **21)** Art. 50 AP-LPD. **22)** Art. 83 al. 4 let. a RGPD.