Annonce des violations de la sécurité des données : une nouvelle obligation de la nLPD

Sylvain Métille* | Pauline Meyer**

The data security principle (art. 8 of the revised Federal Act on Data Protection (rFADP) requires that the controller and when applicable the processor take all the necessary measures to maintain a sufficient level of security when processing personal data, including to prevent any data breach. Nevertheless, data breaches can occur and when so, the controller shall react quickly in order to regain control of the situation. Among the changes brought by the total revision of the FADP, there is a new obligation to notify data breaches, laid down in art. 24 rFADP. In case of a data breach and if the severity threshold has been reached, it shall inform the Federal Data Protection and Information Commissioner (FDPIC) and, under circumstances, the data subjects too. Art. 24 rFADP also provides an obligation for the processor to notify any data breaches to the controller, in order for him to fulfill his obligations. It remains, however, to be seen how this obligation, which can lead to sanctions in case of violation, will be respected once the revised law will be applicable.

Table des matières

I. Introduction

Pour effectuer un traitement de données licite, le responsable du traitement et le sous-traitant doivent respecter les principes fondamentaux de protection des données, dont le principe de sécurité, figurant à l'art. 8 de la Loi fédérale sur la protection des données du 25 septembre 2020 (nLPD).[1] Le principe de sécurité des données peut se diviser en trois composantes : la confidentialité, l'intégrité et la disponibilité des données personnelles.[2] Le responsable du traitement et le sous-traitant doivent donc prendre les mesures techniques et organisationnelles nécessaires pour effectuer un traitement sûr, en évitant qu'une violation de la sécurité n'intervienne durant le traitement des données.[3] En d'autres termes, les mesures prises par le responsable du traitement et le sous-traitant pour garantir la sécurité des données constituent un préalable à la protection de la personnalité de la personne concernée.[4]

Dans l'EEE, le Règlement général sur la protection des données (RGPD)[5] connaît aussi le principe de sécurité et impose au responsable du traitement et

* Professeur associé (Université de Lausanne), Docteur en droit (Université de Neuchâtel), avocat associé (HDC, Lausanne).
** Doctorante, FNS, Maîtrise en droit des professions judiciaires (Université de Lausanne).

1 FF 2020 7397. Le principe de sécurité figurait déjà à l'art. 7 de la Loi fédérale sur la protection des données du 19 juin 1992 (aLPD). Cet article s'intéressant à la nLPD, et par mesure de simplification, il est fait référence à l'aLPD pour la version (encore) en vigueur en 2021. La version actuellement en vigueur est publiée au RS 235.1.

2 Art. 8 al. 1 OLPD ; *Bruno Baeriswyl,* in : Bruno Baeriswyl/Kurt Pärli (éd.), Datenschutzgesetz (DSG), Stämpflis Handkommentar, Berne 2015, pp. 96–97 ; *Philippe Meier,* Protection des données, Fondements, principes généraux et droit privé, Berne 2011, p. 301 N 786 ; *David Rosenthal,* in : David Rosenthal/Yvonne Jöhri (éd.), Handkommentar zum Datenschutzgesetz, Zurich/Bâle/Genève 2008, art. 7 N 13 ; *Christa Stamm-Pfister,* Art. 7 DSG, in : Urs Maurer-Lambrou/Gabor P. Blechta (éd.), Basler Kommentar, Datenschutzgesetz und Öffentlichkeitsgesetz, 3e éd., Bâle 2014, p. 188 s.

3 Art. 8 nLPD ; *Baeriswyl* (n. 2), p. 92.

4 Message du Conseil fédéral concernant la loi fédérale sur la révision totale de la loi fédérale sur la protection des données et sur la modification d'autres lois fédérales du 15 septembre 2017 (cité : Message LPD), p. 6650.

5 Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE.

au sous-traitant qu'ils prennent les mesures techniques et organisationnelles nécessaires pour garantir la sécurité des données personnelles traitées, en tenant compte de l'état des connaissances, des coûts engendrés par ces mesures, des finalités et des risques du traitement.[6] Le RGPD s'applique principalement aux données traitées par des responsables du traitement établis dans l'EEE, mais il peut parfois aussi concerner des entreprises suisses qui visent les résidents de l'EEE en leur fournissant des biens et des services (application extraterritoriale).[7]

Les mesures techniques consistent par exemple en l'authentification par un mot de passe, le chiffrement des données et la réalisation de sauvegardes régulières. Les mesures organisationnelles comprennent par exemple la formation, la documentation, les instructions, les contrats et les contrôles.[8] En pratique, on constate souvent que les mesures techniques ne sont pas suffisamment complétées par les mesures organisationnelles nécessaires.[9]

Parfois les mesures sont inexistantes ou insuffisantes, et des violations de sécurité peuvent se produire. C'est ce qui est arrivé en 2018 lorsque des tiers malintentionnés sont parvenus à soustraire des données personnelles durant une cyberattaque contre la filiale de Swisscom, MyStrom.[10] Aujourd'hui, ces incidents de sécurité sont fréquents et peuvent toucher n'importe quelle entreprise et n'importe quel secteur économique. Certains peuvent être évités facilement en prenant des mesures appropriées en amont[11], alors que d'autres seront inévitables.[12] Il est donc important que des mesures soient prises *a posteriori* également pour limiter les risques causés par la violation et éviter qu'elle ne se reproduise. C'est dans ce but que la nLPD a introduit la notion de violation de la sécurité des données et des obligations d'annonce. Après avoir vu quelques notions importantes (II), nous examinerons les obligations d'annonce du responsable du traitement (III) et du sous-traitant (IV), ainsi que les sanctions (V).

II. Notions

La nLPD définit les violations de la sécurité des données à son art. 5 let. h comme « toute violation de la sécurité entraînant de manière accidentelle ou illicite la perte de données personnelles, leur modification, leur effacement ou leur destruction, leur divulgation ou un accès non autorisés à ces données ».[13] C'est une forme d'incident de sécurité visant des données personnelles et ayant comme conséquence que le responsable du traitement n'est plus capable d'assurer la conformité du traitement avec les principes régissant les traitements de données personnelles.[14]

Il existe plusieurs formes de violations de la sécurité des données selon la composante du principe de sécurité touchée.[15] Premièrement, l'effacement, la destruction et la perte portent atteinte à la disponibilité des données. L'effacement pourrait être la conséquence de l'acte volontaire du responsable du traitement et la destruction celle de l'acte d'un tiers, alors que la perte serait indépendante de tout acte d'une

6 Art. 5 par. 1 let. f RGPD. Voir également les Lignes directrices du Groupe de travail « Article 29 » sur la protection des données sur la notification de violations de données à caractère personnel en vertu du règlement (UE) 2016/679 du 3 octobre 2017, version révisée et adoptée le 6 février 2018 (cité : Lignes directrices Notification G29), pp. 6 s.

7 Art. 3 RGPD. Voir également *Sylvain Métille/Annelise Ackermann,* « RGPD : application territoriale et extraterritoriale », in : Astrid Epiney (éd.), Datenschutzgrundverordnung (DSGVO) : Tragweite und erste Erfahrungen = Le règlement général sur la protection des données (RGPD) : portée et premières expériences, Zürich 2020, pp. 77–97 et les réf. cit.

8 Art. 8 ss OLPD ; *Rosenthal* (n. 2), art. 7 N 8 s.

9 L'exemple classique du mot de passe compliqué inscrit sur un post-it collé sur le bord de l'écran reste malheureusement trop souvent valable.

10 En 2018, la filiale de Swisscom MyStrom a été la cible d'une cyberattaque, au cours de laquelle des cybercriminels sont parvenus à infiltrer des milliers de réseaux locaux sans fil (wlan) en Suisse. Des données sensibles ainsi que des données bancaires ont été exposées ; les pirates ont également réussi à piloter des appareils électroniques à distance et à écouter des conversations téléphoniques sans se faire remarquer, Le Temps, 12 août 2018, <*https://www.letemps.ch/economie/pirates-sattaquent-aux-prises-courant-dune-filiale-swisscom*>.

11 Par exemple des mesures organisationnelles très simples pour s'assurer de la destruction correcte des supports de données.

12 Les responsables de la sécurité informatique disent souvent que la question n'est pas de savoir si une violation de la sécurité aura lieu, mais quand elle aura lieu.

13 Cette définition est semblable à celle des art. 4 ch. 12 RGPD et 15 de la loi fédérale sur la protection des données personnelles dans le cadre de l'application de l'acquis de Schengen dans le domaine pénal (LPDS).

14 *Cornelia Mattig,* Achtung, wir haben eine Datenpanne ! Was nun ?, Expert Focus 6–7/19, pp. 491 ss, p. 491.

15 Message LPD (n. 4), p. 6681.

personne. Malgré la terminologie de la nLPD, il n'y a à notre avis pas de différence fondamentale entre la perte, l'effacement et la destruction des données. Deuxièmement, la modification porte atteinte à l'intégrité des données. Troisièmement, la communication des données à des tiers non autorisés porte atteinte à la confidentialité.

Ces violations peuvent avoir diverses causes. Elles peuvent être d'origine humaine, l'individu étant considéré par sa négligence ou son imprévoyance comme le maillon faible en matière de sécurité, ou technique. De même que la question de l'origine, la question de l'intention ou la négligence n'importe pas dans ce contexte.[16] Ce qui compte c'est que l'atteinte à la sécurité a eu lieu. Peu importe que les données aient été effectivement exploitées. L'ampleur et les conséquences de la violation ne jouent pas un rôle important pour déterminer l'existence d'une violation en tant que telle. Elles sont en revanche déterminantes pour estimer le risque pour les personnes concernées et pour définir les mesures à prendre.[17]

La violation de la sécurité peut être plus ou moins grave: une violation peut être sans risque ou entraîner des risques, voire des risques élevés pour la personnalité et les droits fondamentaux des personnes concernées. Par exemple, si un site de vente de vêtements en ligne est visé par une cyberattaque durant laquelle des données personnelles sont momentanément inaccessibles, il n'y a vraisemblablement pas de risque. En revanche, si elles sont copiées par l'attaquant, il y a une violation susceptible d'entraîner de tels risques. Si les données permettent de causer par exemple une usurpation d'identité, une perte financière ou encore une atteinte à la réputation, on parlera de violation susceptible d'entraîner un risque élevé pour la personnalité et les droits fondamentaux de la personne concernée.[18]

La violation peut être causée par un tiers, mais aussi par un collaborateur du responsable du traitement ou du sous-traitant qui aurait fait preuve de négligence ou qui aurait outrepassé ses compétences. Elle peut entraîner (mais pas obligatoirement) une perte de contrôle, une utilisation abusive des données ou encore des atteintes à la personnalité, comme la divulgation d'informations que la personne concernée souhaitait garder secrètes.[19] Dans son rapport d'activité 2019, la Commission nationale française de l'informatique et des libertés (ci-après: la CNIL) indique que l'origine principale des violations de sécurité serait le piratage: 50% des violations ont été causées par des actes externes malveillants, alors que 23% étaient dues à des actes internes accidentels.[20] Une forte majorité des cas portaient atteinte à la confidentialité des données.[21]

À noter que jusqu'à la révision de la LPD, la seule possibilité pour le Préposé fédéral à la protection des données et à la transparence (PFPDT), en cas de soupçon de violation de la sécurité, était de mener une enquête et émettre des recommandations d'un point de vue du principe de la sécurité; c'est seulement avec l'entrée en vigueur de la nLPD qu'existera un devoir d'information, à certaines conditions.[22] Pour être complet, on précisera encore qu'il existe une obligation de signaler les cyberattaques sur la base de l'art. 29 LFINMA[23], pour les établissements qui sont soumis à la surveillance de la FINMA.[24] À noter que cette obligation s'ajoute à celles de la nLPD et que le

16 *Adrian Bieri/Julian Powell,* Die Totalrevision des Bundesgesetzes über den Datenschutz – Übersicht der wichtigsten Neuerungen für Unternehmen, Jusletter 16 novembre 2020, p. 13.

17 Notamment si une annonce est requise. Message LPD (n. 4), pp. 6642–6643.

18 Exemples tirés des Lignes directrices Notification G29 (n. 6), p. 10. Voir également les nombreux exemples contenus dans les Guidelines 01/2021 on Examples regarding Data Breach Notification v 1.0 du Comité européen de la protection des données (CEPD) adoptées le 14 janvier 2021 (mises en consultation au moment de la rédaction de cet article).

19 Message LPD (n. 4), pp. 6680 s.

20 Rapport d'activité 2019 de la Commission nationale de l'informatique et des libertés, Protéger les données personnelles, Accompagner l'innovation, Préserver les libertés individuelles (cité: Rapport d'activité 2019 CNIL), p. 74. Il ne faut à notre avis pas non plus sous-estimer la négligence du responsable du traitement et ces employés. Ces cas sont peut-être moins connus et donc pas annoncés.

21 Rapport d'activité 2019 CNIL (n. 20), p. 74.

22 Art. 29 aLPD; *Stamm-Pfister* (n. 2), p. 191 s.

23 Loi sur l'Autorité fédérale de surveillance des marchés financiers.

24 Voir à ce sujet la Communication FINMA sur la surveillance 05/2020 Obligation de signaler les cyberattaques selon l'art. 29 al. 2 LFINMA du 7 mai 2020; *Sébastien Fanti,* De l'obligation de signaler les cyberattaques selon l'article 29 al. 2 LFINMA – Communication FINMA sur la surveillance 05/2020, 15 décembre 2020 in <*www.swissprivacy.law/43*> et *Rolf H. Weber/Simon Henseler,* Daten-Governance und Cloud Banking im neuen Datenschutzrechtsumfeld, RSDA 6/2020, pp. 604 ss, p. 608.

responsable du traitement peut être amené à faire deux annonces distinctes à la FINMA et au PFPDT.

III. L'obligation d'annonce du responsable du traitement

1. Dans quels cas ?

Lorsqu'une violation de la sécurité est suspectée, le responsable du traitement doit effectuer une brève enquête en vue de déterminer si une violation a effectivement eu lieu. Cette enquête n'est pas encore détaillée à ce stade, mais il s'agit plutôt de déterminer avec un degré de certitude raisonnable et le plus rapidement possible si une violation s'est bel et bien produite. Si la violation est confirmée ou suffisamment probable, le responsable du traitement doit évaluer les conséquences possibles pour la personnalité des personnes concernées et il peut lui incomber d'annoncer la violation si un certain seuil de gravité est atteint.[25] Cette obligation, qui dépend de la gravité de la violation, s'applique aux responsables du traitement privés et aux organes fédéraux.[26] Pour que le responsable du traitement puisse agir au plus vite après la détection d'une violation de la sécurité, il convient d'avoir préparé et testé des processus clairs à suivre concernant la détection de la violation, la mise en place de mesures correctrices, l'annonce et la collecte d'informations nécessaires.[27]

En droit suisse, seule la violation « entraînant vraisemblablement un risque élevé pour la personnalité ou les droits fondamentaux de la personne concernée » devra être notifiée par le responsable du traitement au PFPDT.[28] Tel est le cas lorsqu'une violation est susceptible d'engendrer des dommages physiques, matériels ou un préjudice moral pour les personnes dont les données ont fait l'objet de la violation.[29] Pour qu'un risque élevé soit admis, il faut qu'un dommage, par exemple un vol, une usurpation d'identité ou encore une discrimination, soit susceptible de se produire.[30] Il n'est en revanche pas nécessaire qu'un certain nombre de personnes soient concernées.[31]

Le responsable du traitement qui notifie chaque violation insignifiante aux personnes concernées prend le risque que ces dernières se désensibilisent et ne prennent plus au sérieux une violation importante de sécurité intervenant par la suite. Toutefois, l'interprétation de l'annonce insignifiante doit être restrictive.[32] En effet, le risque élevé ainsi que son caractère vraisemblable pouvant être difficiles à évaluer, notamment dans les cas individuels, il peut être préférable de signaler une violation de la sécurité plutôt que de la cacher.[33]

À titre de comparaison et contrairement au droit suisse qui prévoit la notification au PFPDT seulement si la violation entraîne un risque élevé, le RGPD prévoit la notification à l'autorité de contrôle dans tous les cas, sauf si la violation n'est pas susceptible d'engendrer un risque pour les droits et libertés de la personne concernée.[34] Il y a donc des violations qui sous l'angle du RGPD devraient être annoncées (il y a un risque pour les personnes concernées) mais pas sous l'angle du droit suisse car s'il y a bien un risque, ce risque n'est pas suffisamment élevé. Tel serait par exemple le cas si un responsable du traitement découvre un défaut dans son site web qui permettrait à certains utilisateurs d'accéder aux données d'autres utilisateurs, mais que ces données ne sont pas sensibles et qu'il n'y a pas de risque élevé pour la personnalité des personnes concernées.

25 Message LPD (n. 4), p. 6681. Une obligation analogue existe en droit européen et elle est prévue aux art. 33 s. RGPD. Le responsable du traitement qui serait soumis à la nLPD et au RGPD devrait alors annoncer la violation au PFPDT (en vertu de la nLPD) et aux autorités européennes compétentes (en vertu du RGPD).

26 Message LPD (n. 4), p. 6681.

27 *Mattig* (n. 14), p. 492.

28 Art. 24 nLPD.

29 Par analogie, Lignes directrices Notification G29 (n. 6), p. 26.

30 Liste d'exemples disponible dans l'avis 03/2014 du Groupe de travail « Article 29 » sur la notification des violations de données à caractère personnel adopté le 25 mars 2014. La notion de risque élevé n'est pas la même que celle qui concerne l'analyse d'impact relative à la protection des données (art. 22 nLPD). Voir également *David Rosenthal,* Das neue Datenschutzgesetz, Jusletter 16 novembre 2020, N 163.

31 Dans le même sens, *Rosenthal* (n. 30), N 162.

32 *Sylvain Métille,* Annoncer les failles de sécurité n'est plus une option. Nouvelles obligations lorsque des données personnelles sont exposées, Expert Focus 11/2017, pp. 863 ss, p. 864 s.

33 *Bieri/Powell* (n. 16), p. 13.

34 Lignes directrices Notification G29 (n. 6), pp. 13 et 34. À noter que si les circonstances évoluent et que le responsable du traitement découvre ultérieurement un tel risque, il devra notifier cette évolution à l'autorité de contrôle et prendre des mesures complémentaires, Lignes directrices Notification G29 (n. 6), p. 21.

Pour évaluer le risque, le responsable du traitement doit considérer, dans une évaluation objective, la probabilité et la gravité du risque pour les droits et libertés des personnes concernées.[35] En effet, des personnes vulnérables telles que les mineurs, les personnes en situation de handicap ou les personnes âgées pourraient être exposées à un plus grand risque d'atteintes. En revanche, le responsable du traitement qui envoie par erreur des données au mauvais département d'un fournisseur avec qui il travaille régulièrement ne sera en principe pas considéré comme ayant créé un risque d'atteinte, vu que l'on peut s'attendre à un certain niveau de fiabilité au sein des différents départements de son fournisseur. De plus, l'incidence de la violation va dépendre, entre autres, de la nature et du caractère des données, du type de la violation, de la facilité d'identification, du nombre de personnes concernées ou encore des caractéristiques particulières du responsable du traitement. Par exemple, le risque pour les personnes concernées sera certainement plus élevé s'il s'agit de données médicales que s'il s'agit d'une liste de diffusion d'un journal. De même, plus le nombre de personnes concernées est élevé, plus les conséquences potentielles d'une violation sont, en principe, nombreuses.[36] À noter qu'en cas de doute, il faudrait logiquement opter pour la prudence et notifier la violation.[37]

Dans cet ordre d'idée, la clinique privée qui apprend qu'un patient a reçu la facture liée à une intervention médicale d'un autre patient et qui découvre un défaut impliquant que d'autres personnes pourraient être affectées, devra notifier cette violation au PFPDT. Les données étant sensibles et un grand nombre de personnes étant potentiellement touchées, la violation est susceptible d'engendrer un risque élevé pour la personnalité et les droits fondamentaux des personnes concernées.

2. À qui ?

2.1 À l'autorité

Le principe est que l'annonce doit être faite par le responsable du traitement au PFPDT. L'objectif poursuivi est celui de permettre à ce dernier d'agir rapidement ou de donner des conseils et de pousser le responsable du traitement à agir rapidement.[38] Les conseils donnés par l'autorité peuvent concerner les mesures à prendre ou encore le message à communiquer aux personnes concernées.

2.2 Aux personnes concernées

Si les conditions de l'art. 24 al. 4 nLPD sont remplies, la violation va devoir être annoncée aux personnes concernées, en plus du PFPDT. Prenons l'exemple d'un responsable du traitement qui gère un marché en ligne. Si une cyberattaque a lieu et le pirate obtient des noms d'utilisateurs, mots de passe et historiques d'achat et les publie en ligne, il y aura un risque élevé pour la personnalité des personnes concernées et le responsable du traitement devra par conséquent les en informer.[39]

La communication de la violation poursuit également un objectif de transparence[40], mais elle vise surtout à permettre que les mesures (que seules les personnes concernées peuvent prendre) puissent être prises rapidement pour limiter les conséquences de la violation de la sécurité.[41]

Ainsi, le responsable du traitement doit se demander si l'information permettrait à l'individu de prendre des mesures tendant à la réduction des risques d'atteinte à sa personnalité ou à ses droits fondamentaux. Tel est le cas si la personne concernée peut di-

35 Plusieurs outils sont disponibles pour aider les responsables du traitement à évaluer ce risque. Voir par exemple le document de travail «Recommandations for a methodology of the assessment of severity of personal data breaches» de décembre 2013 de l'ENISA et *Rosenthal* (n. 30), N 162.

36 *Rosenthal* (n. 30), N 162.

37 Cette affirmation sage doit néanmoins être relativisée car en l'absence de sanction, le droit suisse n'est pas très incitatif et le responsable du traitement pourrait voir toutes sortes d'avantages à rester discrets plutôt qu'à respecter fidèlement ses obligations légales. Ces «avantages» n'en sont souvent plus dès que la violation est connue et l'absence d'annonce peut aussi porter atteinte à l'image du responsable du traitement. Les enjeux ne sont donc pas seulement juridiques.

38 Message LPD (n. 4), p. 6681.

39 *Rosenthal* (n. 30), N 162. Dans un tel cas, il y aura notamment un risque d'usurpation d'identité, de vol et/ou de perte financière pour les personnes concernées.

40 On peut aussi se demander si ce n'est pas une sorte de sanction qui oblige le responsable du traitement à dévoiler ses manquements et à faire amende honorable.

41 Message LPD (n. 4), p. 6681 et *Métille* (n. 32), p. 865. Par ailleurs, la notification est en principe faite auprès de l'autorité en premier, mais, dans des circonstances exceptionnelles, l'annonce aux personnes concernées peut précéder celle faite à l'autorité.

minuer la menace par le biais d'un changement de mot de passe ou de données d'accès, ou encore par la vérification d'un relevé de comptes.[42] Il ne s'agit toutefois pas que de mesures de sécurité. Dans le cas de l'exposition de photos intimes ou documents médicaux, l'information de la personne concernée lui permettra d'anticiper leur éventuelle publication qu'il s'agisse d'organiser une conférence de presse pour une personnalité publique, d'informer préalablement les membres de sa famille, ou simplement d'éviter l'effet de surprise de la personne concernée.

Concernant plus précisément la manière de contacter les personnes concernées, la nLPD ne prévoit rien, mais la communication directe, comme en droit européen, devrait être la règle en Suisse également. Le message, de préférence écrit, ne devrait pas contenir d'autres informations. L'annonce peut s'effectuer par un canal de contact unique comme par plusieurs canaux différents, en vue de maximiser la probabilité que toutes les personnes concernées prennent connaissance de l'information.[43] Si la communication individuelle exige des efforts disproportionnés, le responsable du traitement pourrait agir par le biais d'une communication générique à tous ses clients, voire une communication publique.[44]

Par ailleurs, le responsable du traitement peut envisager des mesures complémentaires à l'annonce, comme une page sur son site web contenant les détails de l'incident ainsi que les étapes à suivre par les personnes concernées afin d'optimiser leur protection.

3. Dans quel délai ?

Le législateur a laissé une marge d'appréciation au responsable du traitement qui doit annoncer la violation au PFPDT « dans les meilleurs délais » selon l'ampleur de la violation et du risque pour la personne. Même si aucun délai n'est prévu pour l'annonce aux personnes concernées, elle doit aussi intervenir au plus vite[45]. Il est évident que plus le risque est important pour la personne concernée ou le nombre de personnes concernées est élevé, plus la violation devra être annoncée rapidement, que ce soit au PFPDT ou aux personnes concernées.[46]

Dans tous les cas, il est nécessaire que le responsable du traitement agisse rapidement et correctement, autrement il prend le risque qu'à la violation de la sécurité s'ajoutent des conséquences dévastatrices pour lui comme pour les personnes concernées, passant des procédures coûteuses aux pertes de clients et à un effondrement de sa réputation.

À l'inverse de la nLPD, le RGPD a fixé un délai précis en exigeant du responsable du traitement d'agir, si possible, dans les 72 heures.[47] Le point de départ du délai de 72 heures prévu par le RGPD correspond au moment où le responsable du traitement est réputé avoir « pris connaissance » d'une violation de la sécurité des données. Ceci est le cas lorsqu'il est « raisonnablement certain qu'un incident de sécurité s'est produit et que cet incident a compromis des données personnelles ».[48] Par exemple, si un responsable du traitement découvre qu'une clé USB contenant des données personnelles a disparu et qu'aucune sauvegarde n'a été effectuée, il serait dans tous les cas confrontés à une violation de la disponibilité et serait réputé en avoir pris connaissance au moment où il s'aperçoit de la disparition de la clé. De même, lorsque le sous-traitant a notifié au responsable du traitement une violation s'étant produite dans sa sphère de contrôle, ce dernier est considéré comme en ayant pris connaissance.[49] Ce moment dépend des circonstances de la violation dans le cas d'espèce, mais il est nécessaire que le responsable du traitement mette en place toutes les mesures techniques et organisationnelles pour établir si une violation a effectivement eu lieu, et cela dans les meilleurs délais.

Les premières heures suivant la prise de connaissance d'une violation de la sécurité sont cruciales et chaque minute compte pour rétablir la sécurité des données et minimiser les risques. Par conséquent, le fait que la nLPD ne fixe pas un délai aussi rigide que les 72 heures exigées par le RGPD pourrait être bénéfique pour les responsables du traitement, en leur permettant de mettre d'abord en place les mesures pour parer à la faille, puis de notifier la violation au

42 Message LPD (n. 4), pp. 6681 s. ; *Rosenthal* (n. 30), N 166.

43 Il faut de plus tenir compte des formats et de la langue appropriés : Lignes directrices Notification G29 (n. 6), p. 24.

44 Dans certains cas, la communication publique sera la seule solution envisageable (par exemple si le responsable du traitement n'a pas de données de contacts ou qu'elles ont précisément été détruites).

45 Voire encore plus vite puisque des mesures doivent être prises par les personnes concernées.

46 Message LPD (n. 4), p. 6681 ; *Métille* (n. 32), p. 865.

47 Art. 33 par. 1 RGPD.

48 Lignes directrices Notification G29 (n. 6), p. 11.

49 Lignes directrices Notification G29 (n. 6), p. 15.

PFPDT. Cela permettrait aussi de mieux établir les faits. En pratique toutefois, le PFPDT risque de s'inspirer du RGPD.

Si une annonce aux personnes concernées est nécessaire, elle devra intervenir rapidement et il nous semble dans ce cas beaucoup plus difficile de dépasser, *grosso modo,* les 72 heures. Quoiqu'il en soit, il est conseillé aux responsables du traitement de prévoir des procédures et des modèles standards.[50]

4. Que faut-il annoncer?

L'art. 24 al. 2 nLPD pose des exigences minimales relatives au contenu de l'annonce au PFPDT. Le responsable du traitement doit y faire figurer le type ou la nature de la violation (effacement/destruction, perte, modification ou communication à un tiers non autorisé), ainsi que ses conséquences sur la personne concernée et les mesures prises ou envisagées en vue d'arranger la situation ou du moins en réduire les conséquences négatives.[51] Si certaines informations ne sont pas disponibles, une information échelonnée est envisageable.

De nombreuses autorités européennes de protection des données ont publié des formulaires à l'attention des responsables du traitement établis sur leur territoire et l'on peut s'attendre à ce que le PFPDT en fasse de même. L'ordonnance dressera la liste des éléments devant obligatoirement figurer dans l'annonce. Le responsable du traitement devrait faire figurer dans son annonce la chronologie des événements en lien avec la violation de la sécurité, la cause de la violation (si elle est déjà constatable) ou encore des précisions sur l'aspect transfrontalier du traitement s'il y en a un.[52] Plus l'annonce est complète et transparente, mieux le responsable du traitement satisfait à son obligation et évite des complications avec l'autorité de contrôle pour la suite. Il y aura néanmoins souvent des informations qu'il n'aura pas envie de partager, qu'il s'agisse de secrets d'affaires ou d'éléments laissant penser à d'autres violations de la nLPD. Parfois même le responsable du traitement pourrait être tenté de ne pas contacter le PFPDT, considérant qu'il a plus «à perdre».[53] De tels choix sont plus probables en droit suisse qu'en droit européen vu l'absence de sanctions directes dans la nLPD pour défaut d'annonce.[54]

Pour ce qui est en revanche du contenu de l'annonce aux personnes concernées, la nLPD ne prévoit rien, contrairement à l'art. 34 par. 2 RGPD qui précise que la nature de la violation ainsi que ses conséquences probables doivent, comme pour l'annonce à l'autorité, y figurer, de même que les mesures prises par le responsable du traitement pour limiter les conséquences négatives. De plus, le responsable du traitement doit transmettre les coordonnées de la personne à contacter, pour permettre aux personnes concernées de poser des questions ou de réagir au mieux. Finalement, le responsable du traitement doit compléter sa notification par des recommandations à l'attention des personnes concernées afin qu'elles puissent prendre les mesures qui s'imposent pour se protéger.[55] Ces éléments figureront dans l'ordonnance. Si tel n'est pas le cas, le responsable du traitement ferait bien de s'en inspirer.

5. Les exceptions

Il existe plusieurs situations lors desquelles il n'est pas nécessaire d'annoncer des violations de sécurité au PFPDT (et aux personnes concernées). C'est premièrement le cas lorsque le seuil de gravité ou le risque induit par la violation n'est pas atteint. Lorsque la violation peut être considérée comme insignifiante, le responsable du traitement n'aura pas à l'annoncer, ni au préposé, ni à la personne concernée.[56]

50 *Bieri/Powell* (n. 16), p. 13.

51 Message LPD (n. 4), p. 6681; *Rosenthal* (n. 30), N 164.

52 Voir par exemple le formulaire complet de la Commission nationale luxembourgeoise de protection des données, accessible sous: *<https://cnpd.public.lu/fr/professionnels/obligations/violation-de-donnees/violation-donnees-rgpd.html#>;* voir également le formulaire anglais, accessible sous: *<https://ico.org.uk/for-organisations/report-a-breach/personal-data-breach/>*.

53 En particulier si l'annonce au PFPDT devait conduire à l'ouverture d'une enquête et des mesures administratives, ou si l'annonce aux personnes concernées devaient leur faire prendre connaissance de traitements qu'elles n'imaginaient pas et auxquels elles pourraient s'opposer.

54 Voir le chapitre V. Les sanctions ci-dessous.

55 Lignes directrices Notification G29 (n. 6), p. 23.

56 Message LPD (n. 4), p. 6681; tel pourrait être le cas notamment lorsque des données disponibles pour le public sont divulguées. De même dans le cas d'une violation de confidentialité portant sur des données cryptées, si une copie de ces données réside chez le responsable du traitement. À noter que la situation, si elle évolue, devra être réévaluée par le responsable du traitement.

Par exemple, une interruption de réseau de quelques minutes dans un centre d'appels ne sera pas susceptible d'entraîner de risques et ne devra donc être annoncée à personne.[57] C'est aussi le cas, lorsque la violation, sans être insignifiante n'est que susceptible d'engendrer un risque qui n'est pas élevé pour la personnalité et les droits fondamentaux de la personne concernée. Dans ce cas également, même s'il y a une violation de la sécurité, elle ne déclenche pas d'obligation d'annonce au sens de l'art. 24 nLPD.[58]

Deuxièmement, c'est le cas lorsque les données concernées ne sont pas des données personnelles. Il n'y a alors pas de violation de la sécurité des données au sens de la nLPD. Il n'y a pas non plus d'obligation d'annoncer une violation de la sécurité lorsque les données sont chiffrées et qu'elles ne peuvent raisonnablement pas être déchiffrées.[59] En effet, ces données anonymes ne sont pas des données personnelles au sens de l'art. 5 let. a nLPD.

On trouve ensuite des exceptions à l'obligation d'informer les personnes concernées, alors même que la violation représente un risque suffisamment important pour justifier en temps normal une information. Ces exceptions ne modifient pas l'obligation d'informer le PFPDT. À la lecture de l'art. 24 al. 5 nLPD, le responsable du traitement peut renoncer, restreindre ou différer l'annonce du traitement non autorisé à la personne concernée si un devoir de garder le secret l'en interdit, si l'on se trouve dans un cas où des intérêts prépondérants d'un tiers l'exigent ou, si le responsable du traitement est un organe fédéral, qu'un intérêt public prépondérant existe ou que la communication des informations est susceptible de compromettre une enquête ou procédure judiciaire.[60]

De même, l'annonce aux personnes concernées peut être omise si elle implique des efforts disproportionnés ou qu'elle est impossible à entreprendre. Si l'information individuelle ne permet pas d'améliorer sensiblement l'information de la personne concernée, le responsable du traitement peut annoncer la violation aux personnes concernées par le biais d'une communication publique. Tel est le cas si le responsable du traitement n'est pas en mesure d'identifier les personnes concernées par le traitement non autorisé car, par exemple, des fichiers journaux permettant une identification ne sont plus disponibles. La situation est la même si les coûts résultant d'une information individuelle à un grand nombre de personnes semblent excessifs en comparaison à ce que gagneraient les personnes concernées de l'information (art. 24 al. 5 let. c nLPD).[61]

Rosenthal considère qu'aucune annonce aux personnes concernées n'est due lorsque ces dernières ont antérieurement déclaré leur désintérêt quant à cette annonce.[62] Nous ne partageons pas cet avis, l'obligation légale de l'art. 24 al. 4 nLPD s'imposant au responsable du traitement indépendamment de la volonté de la personne concernée. Par analogie avec les exigences applicables au consentement, il sera dans la plupart des cas douteux que la personne concernée puisse disposer à l'avance des informations suffisantes pour évaluer l'intérêt d'être informée et d'y renoncer en toute connaissance de cause.

Finalement, on doit encore admettre qu'il n'y a pas d'obligation pour le responsable du traitement de notifier une violation aux personnes concernées s'il a pris les mesures techniques et organisationnelles appropriées pour protéger les données personnelles compromises, immédiatement après la violation par exemple en bloquant les accès et évitant que les données exposées ne soient exploitables.[63] L'annonce à la personne concernée n'est généralement pas nécessaire à sa protection et, partant, le responsable du traitement n'aurait à annoncer la violation de la sécurité à celle-ci que sur injonction du PFPDT.[64] Une information au PFPDT sera en revanche due car il y a bien eu un risque élevé pour les personnes concernées, même si c'était seulement pendant une durée limitée.

57 Pour d'autres exemples, voir *Rosenthal* (n. 30), N 162.

58 Art. 24 al. 1 et 4 nLPD ; art. 33 par. 1 et 34 par. 1 RGPD *a contrario*. Dans un tel cas, une notification serait due en application du RGPD.

59 *Métille* (n. 32), p. 865.

60 Art. 24 al. 5 nLPD, qui renvoie à l'art. 26 al. 1 let b et al. 2 let b nLPD.

61 Message LPD (n. 4), p. 6682.

62 *Rosenthal* (n. 30), N 162. Il admet pourtant que le sous-traitant et le responsable du traitement ne peuvent pas déroger à l'obligation d'annoncer (*Rosenthal* [n. 30], N 165*)*.

63 Si les mesures étaient prises avant la violation, par exemple par le biais d'un chiffrement de haut niveau il n'y aurait pas de risque élevé (voire pas de données personnelles) et donc pas d'obligation non plus d'annoncer au PFPDT.

64 Art. 24 al. 4 nLPD.

IV. L'obligation d'annonce du sous-traitant[65]

Le sous-traitant a comme mission générale de traiter les données pour le compte et selon les instructions du responsable du traitement.[66] Cela implique aussi de l'aider à respecter ses obligations légales et contractuelles. Si une violation de la sécurité intervient chez le sous-traitant, il est tenu de la notifier au responsable du traitement, dans les meilleurs délais.[67] Contrairement au responsable du traitement, le sous-traitant doit annoncer une violation de la sécurité indépendamment du risque. En d'autres termes, la violation ne doit pas atteindre un certain seuil de gravité pour que le sous-traitant doive l'annoncer au responsable du traitement; toute violation avérée doit être annoncée et ce sera au responsable du traitement d'évaluer le risque susceptible d'être engendré par celle-ci.[68]

L'obligation principale incombant au sous-traitant, lorsqu'il découvre qu'une violation a eu lieu dans son domaine de responsabilité, est de l'annoncer au responsable du traitement dans les meilleurs délais. Lorsqu'il n'y a pas de mesure à prendre ni de risque élevé, on sera moins exigeant sur le délai d'annonce. Une fois que le sous-traitant aura informé le responsable du traitement de la violation de la sécurité, ce dernier effectuera, comme lorsque la violation se manifeste chez lui, un examen des risques potentiels afin de décider si la violation doit être notifiée au PFPDT et éventuellement à la personne concernée.[69]

Bien qu'il puisse être désagréable pour un sous-traitant de devoir annoncer chaque violation au responsable du traitement, il s'agit d'une obligation légale qui s'applique en l'absence de disposition contractuelle spécifique et à laquelle il ne peut pas déroger par contrat.[70] Cela se justifie également par le devoir d'instruction et de surveillance du responsable du traitement sur le sous-traitant.[71] La conséquence directe est que le responsable du traitement risque de recevoir de nombreuses annonces de violation de la sécurité des données pour des cas qui ne nécessitent pas d'annonce. L'aspect positif est que cela lui permettra néanmoins de juger de la qualité du travail du sous-traitant. L'aspect négatif est que s'il est mal organisé, il risque de devenir moins sensible aux annonces et oublier de réagir lorsqu'il devrait.

Même si la nLPD ne le précise pas, on peut admettre que si un sous-traitant lié à plusieurs responsables du traitement subit une violation de la sécurité des données en impactant plus d'un, il devra la communiquer à tous les responsables du traitement affectés par la violation.[72]

Le sous-traitant doit agir sans délai dans le but d'aider le responsable du traitement à prendre les mesures nécessaires pour diminuer les conséquences de la violation et respecter son délai d'annonce.

Le responsable du traitement et le sous-traitant peuvent également prévoir dans le contrat de sous-traitance une délégation de compétence pour que le sous-traitant puisse annoncer directement ou sur instruction à l'autorité de contrôle ou aux personnes concernées une violation de la sécurité intervenue dans sa sphère de compétences. En pratique c'est assez rare, car le responsable du traitement souhaite maîtriser cette communication. On trouve plus généralement une clause qui interdit au sous-traitant de communiquer directement, et parfois une possibilité, au cas par cas, pour le responsable du traitement de mandater le sous-traitant pour procéder à une annonce.

V. Les sanctions

Le fait de ne pas annoncer une violation de la sécurité n'est pas directement sanctionné pénalement.[73] Le PFPDT a toutefois la possibilité, sur la base de l'art. 51 al. 3 let. f nLPD, d'ordonner au responsable du traitement, organe fédéral ou responsable du traitement privé, de respecter son obligation d'annonce selon l'art. 24 nLPD et donc d'informer les personnes

65 À noter que le RGPD prévoit également, contrairement à la LPD, le régime de la responsabilité pour les responsables du traitement conjoints, lesquels doivent définir à qui reviendra les obligations découlant des art. 33 s. RGPD, Lignes directrices Notification (n. 6), p. 14.

66 Le sous-traitant est défini à l'art. 5 let. k nLPD.

67 Art. 24 al. 3 nLPD.

68 Message LPD (n. 4), p. 6681.

69 *Métille* (n. 32), p. 865.

70 Dans le même sens *Rosenthal* (n. 30), N 165.

71 Qui est évidemment beaucoup plus étendu que celui du PFPDT sur le responsable du traitement.

72 Par analogie: Lignes directrices Notification G29 (n. 6), p. 15.

73 Dans le même sens: *Rosenthal* (n. 30), N 167.

concernées d'une violation de la sécurité des données. Il s'agit d'une mesure administrative, dont le non-respect par le responsable (privé) du traitement peut être sanctionné pénalement,[74] en vertu de l'art. 63 nLPD. La sanction directe prévue par l'avant-projet de loi sous l'angle de la violation du devoir de renseigner, déclarer et collaborer (art. 50 AP-LPD) n'a pas été conservée.[75] La nLPD ne prévoit donc pas, contrairement au RGPD, la possibilité pour l'autorité de contrôle d'infliger une amende administrative. C'est regrettable. Si le responsable du traitement se soustrait à son obligation d'annoncer, la seule possibilité serait que le PFPDT lui ordonne d'abord de s'y conformer et assortisse sa décision de la menace d'une amende en cas d'insoumission de la part du responsable, puis dénonce le cas aux autorités pénales. Alors seulement une sanction pénale pourrait être envisagée.[76]

Le responsable du traitement ne respectant pas son obligation d'annoncer une violation de la sécurité ne sera passible d'une amende allant jusqu'à CHF 250 000 que dans le cas très limité où il ne respecterait pas la décision du PFPDT lui ordonnant d'annoncer la violation sur la base de l'art. 63 nLPD. Ce n'est donc pas le défaut d'annoncer qui est sanctionné, mais l'insoumission à une décision de l'autorité. À titre de comparaison, l'amende administrative pour défaut d'annonce prévue par l'art. 83 par. 4 let. a RGPD peut s'élever jusqu'à EUR 10 000 000 ou 2% du chiffre d'affaires annuel mondial total de l'entreprise.[77] Pour trouver la juste mesure, l'autorité de contrôle doit être attentive au principe de proportionnalité, et la mesure doit être efficace et dissuasive.[78]

La sanction prévue par l'art. 63 nLPD s'applique uniquement aux responsables du traitement (ou sous-traitants) privés mais non aux organes fédéraux, contrairement aux sanctions prévues par le RGPD. La raison de cette différence réside d'une part dans la confiance portée par le législateur dans les organes fédéraux. D'autre part, et contrairement à certains États européens, il existe en Suisse des procédures séparées visant les organes fédéraux, comme les procédures de responsabilité de l'État. À noter que si le responsable du traitement est un organe fédéral, la personne concernée pourra agir en responsabilité de l'État, si les conditions de l'art. 3 de la Loi du 14 mars 1958 sur la responsabilité de la Confédération, des membres de ses autorités et de ses fonctionnaires (LRCF) sont réunies.[79]

Le responsable du traitement privé peut, en parallèle de la sanction de l'art. 63 nLPD, engager sa responsabilité privée. S'il a manqué à ses obligations contractuelles, il peut engager sa responsabilité sur la base du droit des obligations.[80] L'entreprise qui découvre une violation de la sécurité et qui n'en informe pas ses clients concernés, alors qu'ils auraient pu mettre en œuvre certaines mesures, comme le changement de leurs mots de passe, pourrait être tenue responsable du dommage causé.[81]

Si le responsable du traitement est une entreprise, ce sont les personnes occupant une fonction dirigeante qui engagent leur responsabilité pénale, et non pas l'entreprise (comme c'est le cas pour les sanctions administratives prévues par le RGPD).[82]

Le responsable du traitement engagé dans une procédure pénale peut voir l'obligation d'annoncer entrer en conflit avec son droit de ne pas s'auto-incriminer. Dans de telles situations, il convient de se rappeler l'art. 24 al. 6 nLPD, qui prévoit qu'une annonce de violation de la sécurité ne peut être utilisée dans une procédure pénale dirigée contre la personne à

74 Message LPD (n. 4), p. 6708.

75 Message LPD (n. 4), p. 6717.

76 Message LPD (n. 4), p. 6718 ; le PFPDT aboutit à sa décision d'après une enquête sur la base de l'art. 51 al. 3 let. f nLPD.

77 *Mattig* (n. 14), p. 492 ; Lignes directrices Notification G29 (n. 6), p. 6.

78 Lignes directrices du Groupe de travail « Article 29 » sur la protection des données sur l'application et la fixation des amendes administratives aux fins du règlement (UE) 2016/679 adoptées le 3 octobre 2017 (cité : Lignes directrices Amendes administratives G29), pp. 6 et 18.

79 Voir à ce sujet : *Tobias Jaag,* Le système général du droit de la responsabilité de l'État, in : Anne-Christine Favre/Vincent Martenet/Étienne Poltier (éd.), La responsabilité de l'État, Genève/Zurich/Bâle 2012, pp. 27–36 ; La personne concernée subissant un dommage découlant d'une violation de l'obligation d'annoncer une violation de la sécurité des données devra dès lors agir contre l'État, qui pourra se retourner contre le fonctionnaire par le biais d'une action récursoire, dans le cas où celui-ci aura causé le dommage, soit intentionnellement, ou, dans la majorité des cas probablement, par négligence grave.

80 Selon la loi fédérale complétant le Code civil suisse du 30 mars 1911 (Livre cinquième : Droit des obligations).

81 Si les conditions légales sont réunies. L'absence d'information ne serait pas tellement la cause du dommage, mais plutôt un défaut de prendre des mesures pour éviter ou réduire le dommage.

82 Message LPD (n. 4), p. 6715.

qui incombe le devoir d'annonce qu'avec son consentement, expression du principe *nemo tenetur*. Cette norme vaut pour le responsable du traitement comme pour le sous-traitant.[83]

VI. Conclusion

L'obligation d'annoncer les violations de la sécurité des données est une obligation nouvelle pour un grand nombre d'entreprises. Les sous-traitants doivent annoncer toutes les violations, alors que les responsables du traitement ne doivent annoncer au PFPDT que les violations qui représentent un risque élevé pour les personnes concernées. Dans certains cas encore plus limités, ils devront informer ces personnes directement.

Du point de vue pratique, les entreprises devront réagir très vite afin de limiter les risques créés par la violation, mais également pour déterminer si elles doivent procéder ou non à une annonce, ce qui implique d'avoir en main toutes les informations nécessaires. Pour y arriver, il n'y a guère d'autres options que d'avoir préalablement établi et testé un processus de gestion des incidents.

Du point de vue juridique, les obligations de la nLPD sont moins sévères que celles du RGPD, et surtout les sanctions en cas de silence du responsable du traitement sont quasi inexistantes. Il sera donc particulièrement intéressant de voir comment les entreprises suisses vont réagir: comme leurs voisines européennes en sur-annonçant les violations, ou au contraire en préférant se taire vu le peu d'incitations.

[83] Message LPD (n. 4), p. 6682.