www.jusletter.ch

David Rosenthal, Samira Studer/Alexandre Lombard (pour la traduction)

La nouvelle loi sur la protection des données

Le 25 septembre 2020, le Parlement a adopté la nouvelle Loi fédérale sur la protection des données (nLPD). Elle vise à aligner la protection des données suisses sur celle de l'UE. Toutefois, la nLPD s'écarte du Règlement européen général sur la protection des données (RGPD) sur certains points et va même au-delà de celui-ci à certains endroits. Cet article explique et commente en détail les modifications apportées à la LPD qui sont pertinentes pour le secteur privé, répond aux questions les plus importantes et explique ce qu'elles signifient pour la pratique.

Catégories d'articles : Articles scientifiques
Domaines juridiques : Protection des données ; Droit administratif ; Droit public ; Droit pénal

Proposition de citation : David Rosenthal, Samira Studer/Alexandre Lombard (pour la traduction), La nouvelle loi sur la protection des données, in : Jusletter 16 novembre 2020

Table des matières

I. Introduction

[1] Un an et demi après le message du Conseil fédéral, les Chambres fédérales ont enfin remis l'ouvrage sur le métier : la navette entre les Chambres a dans un premier temps donné lieu à un assouplissement du projet du Conseil fédéral par le Conseil national, s'agissant de certains points, avant que le Conseil des Etats ne resserre la vis une nouvelle fois lors de la session d'hiver 2019. La crainte que la Commission européenne ne reconnaisse pas l'« adéquation » de la Suisse a conduit à des propositions quelque peu drastiques. Cette crainte, à l'évidence exagérée, témoigne d'une certaine propension helvétique à l'obéissance anticipée. Fort heureusement, les parlementaires n'ont pas accepté les modifications les plus radicales issues de leurs propres rangs. Ils n'ont cependant pas pu empêcher la gauche et les partis bourgeois de s'affronter, notamment sur la question du profilage. En définitive, c'est bien la conférence de conciliation qui a permis d'éviter l'échec de la révision totale de la loi. Il s'agissait toutefois, comme nous l'expliquerons plus loin, d'un différend qui ne méritait pas le débat.

[2] Quoi qu'il en soit, le résultat est une LPD révisée qui, bien qu'elle adopte certaines des dispositions les moins judicieuses du RGPD, sera en grande partie relativement facile à mettre en œuvre – même si l'effort requis pour assurer le respect de la protection des données continuera à augmenter dans les années à venir. Par exemple, le devoir d'informer de la nLPD est plus raisonnable que celui du RGPD, l'obligation d'annoncer les violations de la sécurité des données est moins excessive et les exigences relatives au consentement restent raisonnables, contrairement à celles du RGPD. En outre, certaines dispositions de la nLPD sont beaucoup plus souples que celles du RGPD, en particulier celles relatives aux exportations de données. Elles pourront donc être appliquées de manière plus sensée en fonction des circonstances. Bien que les dispositions pénales de la nLPD soient sévères (parce qu'elles sont de nature personnelle), elles s'appliqueront dans bien moins de cas que les amendes élevées infligées aux entreprises dans le cadre du RGPD. La réglementation européenne en matière de « cookies », qui est toujours régie par la Directive vie privée et communications électroniques[1], n'a quant à elle pas été adoptée par la Suisse dans le cadre de la révision (et son adaptation en droit suisse n'est pas prévue pour le moment).

[3] Le projet législatif a également donné lieu à l'édiction de dispositions questionnables et à des compromis politiques peu attrayants, même si certains d'entre eux étaient probablement dus aux exigences du droit européen. Les dispositions problématiques et les occasions manquées concernent notamment le devoir d'informer (encore plus de déclarations de protection des données que presque personne ne lit), le conseiller à la protection des données (dont la mise en œuvre manque d'incitations juridiques concrètes), l'obligation d'annoncer les violations de la sécurité des données (pas de règlementation « *de minimis* »), le droit d'accès et de rectification (dans les deux cas, des lacunes délicates figurent dans les exceptions), la portabilité des données (une réglementation inachevée qui risque d'entraîner beaucoup d'efforts inutiles et des conséquences

1 Directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données personnelles et la protection de la vie privée dans le secteur des communications électroniques.

non voulues), ainsi que le profilage susmentionné, sujet brûlant de la révision. S'agissant de ce dernier terme, il appert que certains parlementaires ne comprenaient pas réellement le concept sous-jacent à cette réglementation. Bien que le Parlement ait passé de nombreux mois à débattre sur la définition juridique du profilage « à risque élevé », il n'a pas prêté attention aux conséquences juridiques de ce profilage. Le conseiller national Cédric Wermuth l'a très bien exprimé lors d'un débat en septembre 2020 à l'occasion duquel il se prononçait sur l'absence de conséquences juridiques : « On pourrait aussi bien définir dans la loi ce qu'est un babouin bleu – cela aurait exactement le même effet que ce que voulait le parti bourgeois »[2]. La proposition précitée n'a, fort heureusement, pas été suivie, mais il n'en demeure pas moins que la version révisée du concept de profilage ne change presque rien au droit actuel. Nous y reviendrons.

[4] L'**entrée en vigueur** de la nLPD est actuellement prévue pour 2022, voire même pour l'été 2022, selon les derniers sons de cloches de la Berne fédérale. La Commission européenne, qui devrait bientôt se prononcer sur le renouvellement de sa décision d'adéquation pour la Suisse, pourrait également avoir son mot à dire à ce sujet. *[La nLPD n'a pas fait l'objet d'un référendum.]* Aucune période de transition n'est par ailleurs prévue (N 200). Dans une prochaine étape, le Conseil fédéral rédigera les ordonnances révisées et les soumettra à la consultation. Ces ordonnances devraient contenir plus de détails sur les nouvelles dispositions – comme par exemple le devoir d'informer – qui, bien entendu, ne pouvaient pas encore être prises en considération lors de la rédaction de cet article.

[5] Les commentaires qui suivent sont basés sur une analyse approfondie de la nLPD vue également sous l'angle de la pratique et de la doctrine afférentes au RGPD. Une version complète de cette analyse paraîtra prochainement sous la forme d'une nouvelle édition du commentaire détaillé de la LPD *[en allemand]* par le soussigné et d'autres co-auteurs. Partant, le lecteur piqué dans sa curiosité est invité à prendre son mal en patience et est renvoyé au commentaire à paraître pour le surplus. En outre, seules les dispositions relatives aux personnes privées sont abordées ici, à l'exclusion de celles relatives aux organes fédéraux.

[6] Soulignons enfin que cet article se réfère à la numérotation des articles du texte soumis au vote final[3]. Une comparaison synoptique pratique est disponible en allemand sur datenrecht.ch, de même qu'une traduction anglaise de la nLPD. *[Une comparaison synoptique pratique est également disponible en français sur swissprivacy.law.]* Différents formulaires d'auto-évaluation du respect de la protection des données sont disponibles sur dsat.ch et sont en cours d'actualisation sur la base du texte soumis au vote final.

---

2 Traduction libre. Le texte original en langue allemande se lit comme suit : « Man könne in das Gesetz auch reinschreiben, was ein blauer Pavian sei – das hätte genau die gleiche Wirkung wie das, was die Bürgerlichen wollten », CN Wermuth, session d'automne 2020, 17 septembre 2020, *[le texte définitif du bulletin officiel est désormais disponible]*.

3 Message 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, https://www.admin.ch/opc/fr/federal-gazette/2017/6565.pdf (état au 9 mars 2021), FF 2017 6565.

II. Admissibilité du traitement des données

A. Les principes de base restent inchangés

[7] La bonne nouvelle tout d'abord : les **principes de bases de la LPD** restent inchangés dans la nLPD. Dans le secteur privé, la règle selon laquelle ni le consentement, ni aucun autre motif justificatif n'est nécessaire pour le traitement des données personnelles reste d'actualité. Un motif justificatif n'est nécessaire que si les principes de traitement (art. 6 et 8 nLPD) ne sont pas respectés, si la personne concernée s'est expressément opposée au traitement (art. 30 al. 2 let. b nLPD) ou si des données sensibles[4] sont communiquées à un tiers (art. 30 al. 2 let. c nLPD).

[8] A cet égard, la LPD diffère considérablement du RGPD. Selon le RGPD, les données personnelles visées aux art. 6, 9 et 10 ne peuvent être traitées que s'il existe une « **base juridique** » de traitement. La nLPD ne connaît de réglementation similaire que pour le traitement des données personnelles par des organes fédéraux. Comme les principes de traitement n'ont pas changé en substance avec la révision, les traitements de données qui étaient (et sont) déjà conformes à la LPD n'auront pas besoin d'être adaptés à la nLPD.

[9] A ce stade, il convient de souligner que la nLPD **ne consiste pas en une simple mise en œuvre du RGPD** et que – en dehors de l'espace Schengen – la Suisse n'est pas obligée de le faire. Ce que la Suisse doit mettre en œuvre est la Convention 108 révisée du Conseil de l'Europe[5], qui a déjà été signée par le Conseil fédéral et dont la ratification a également été approuvée par le Parlement[6]. La plupart des modifications de la LPD sont basées sur la mise en œuvre de la Convention 108 révisée. Seul le droit à la remise et à la transmission des données personnelles émane exclusivement du RGPD. Un examen plus approfondi démontre que si la nLPD s'inspire du libellé du RGPD, elle s'en écarte également à certains égards. Dans la plupart de ces cas, les dispositions de la nLPD vont moins loin, sont moins formalistes ou moins détaillées que celles du RGPD. Dans quelques cas, toutefois, la nLPD est plus stricte que le RGPD[7]. Les entreprises qui sont déjà conformes au RGPD pourront s'appuyer sur leurs travaux de mise en œuvre précédents pour le RGPD, mais ne pourront en principe pas se passer de certains contrôles et travaux de mise en œuvre supplémentaires.

[10] Le RGPD et la pratique existante dans ce domaine auront certainement un impact significatif sur l'**interprétation et l'application de la nLPD**. En effet, le RGPD est déjà en vigueur depuis mai 2018. Partant, on dispose déjà d'expérience(s), d'avis doctrinaux, ainsi que des premières décisions des autorités et des tribunaux. Toutefois, la prudence est ici de mise : ce qui s'applique au RGPD ne s'applique pas nécessairement à la LPD, même en présence de dispositions similaires. Lors des débats parlementaires, il a été souligné à plusieurs reprises que la nLPD devait « se rap-

4 Définition à l'art. 5 let. c nLPD : la mention additionnelle de « profil de la personnalité » a été supprimée.

5 Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, RS 0.235.1.

6 Parlement, session d'été 2020, 19 juin 2020 (https://www.parlament.ch/fr/ratsbetrieb/amtliches-bulletin/amtliches-bulletin-die-verhandlungen?SubjectId=49459 (état au 9 mars 2021)).

7 Par exemple, dans le cadre du champ d'application matériel (art. 2 nLPD), du devoir d'informer (art. 19 nLPD), du droit d'accès (art. 25 nLPD) et des sanctions personnelles, y compris le secret professionnel. Le RGPD ne connaît pas de sanctions personnelles et les dispositions y relatives dans la nLPD ont probablement aussi échappé à beaucoup de personnes en Suisse (art. 60 ss nLPD). La définition de données personnelles sensibles va également plus loin que celle dans le RGPD.

procher » du RGPD[8] et être « compatible »[9] ou « équivalente »[10] à celui-ci, qu'elle devait être « très proche du RGPD »[11], mais qu'elle ne devait pas être une « reprise du RGPD »[12]. La majorité a aussi souligné qu'il fallait éviter un « Swiss finish » (positif), c'est-à-dire que la LPD ne devrait pas être *plus stricte* que le RGPD[13].

[11] Il faut s'attendre à ce que la jurisprudence de la CJUE relative au RGPD et les avis des autorités européennes de protection des données aient un plus grand impact en Suisse que la jurisprudence relative à la précédente Directive européenne sur la protection des données, qui n'a pas reçu beaucoup d'attention en Suisse. Il faut aussi s'attendre à ce que certains responsables du traitement, conseillers et autorités en Suisse adoptent sans réserve les points de vue développés dans le cadre du RGPD (p. ex. des autorités étrangères de protection des données ou des auteurs de commentaires du RGPD) dans le droit suisse, pour des motifs de prudence. Il en résultera certainement un alignement de la LPD sur le RGPD, même là où la réglementation suisse aurait été moins stricte en soi que celle du RGPD. Cette **tendance (prévisible) à l'harmonisation de la LPD et du RGPD** peut présenter des avantages dans la mise en œuvre pratique et peut également être justifiée parce qu'elle simplifie le travail. Cependant, elle contredit la volonté du législateur et atteint ses limites lorsqu'il s'agit d'évaluer des cas individuels ou de déterminer les limites exactes de ce qui est encore légalement autorisé par la LPD. C'est le cas, par exemple, des litiges et des enquêtes placés sous l'égide du Préposé fédéral à la protection des données et à la transparence (PFPDT). Dans ces situations en particulier, il ne faudra pas se contenter d'adopter la doctrine et la pratique relatives au RGPD pour interpréter la LPD. La LPD n'est, dans de nombreux domaines, pas qu'une simple version réduite du RGPD, même si elle contient des dispositions comparables. Il existe, en outre, des différences conceptuelles entre les dispositions de la LPD et du RGPD, notamment en ce qui concerne le moment précis où le devoir d'informer doit être respecté ou la manière dont une objection au traitement par les personnes concernées doit être traitée. La Suisse dispose de sa propre loi sur la protection des données et devrait l'appliquer en conséquence. De cette manière, les excès en matière de protection des données et les « conséquences non voulues » du droit européen – lesquels ont été critiqués à plusieurs reprises par différents partis lors des débats parlementaires – pourront être évités en Suisse.

[12] Ces observations sont d'autant plus vraies que le RGPD vise non seulement des concepts réglementaires différents (« règle d'interdiction », N 8), mais va également plus loin que la LPD en termes de finalité. Le RGPD protège à la fois la personnalité des personnes concernées et les « libertés fondamentales ». Ce concept de droit européen n'existe toutefois pas en Suisse. Ainsi, le RGPD protège non seulement contre les discriminations exercées par l'État, mais aussi contre les discriminations exercées par des personnes privées – aspect qui doit être pris en compte lors de l'application des normes pertinentes. La LPD, en revanche, n'a pas vocation à protéger les libertés fondamentales et ne contient donc aucune protection contre la discrimination. Bien que certaines dispositions de la LPD mentionnent la **protection des droits fondamentaux** en sus de la

8 CF Keller-Sutter, BO 2019 N 1782, session d'automne 2019, 24 septembre 2019.

9 CE Fässler, BO 2019 N 1239, session d'hiver 2019, 18 décembre 2019.

10 CN Romano, BO 2019 N 1778, session d'automne 2019, 24 septembre 2019 ; CN Glättli, BO 2019 N 1814, session d'automne 2019, 25 septembre 2019.

11 CN Jauslin, BO 2019 N 1775, session d'automne 2019, 24 septembre 2019.

12 CN Wermuth, BO 2019 N 1777, session d'automne 2019, 24 septembre 2019.

13 CN Romano, BO 2019 N 1802 ; CN Fluri, BO 2019 N 1782 ; BR Keller-Sutter, BO 2019 N 1789 ; CN Flach, CN Brunner, BO 2019 N 1800, session d'automne 2019, 24 septembre 2019.

protection de la personnalité (p. ex. l'art. 22 al. 1 nLPD), cette référence concerne exclusivement les cas où des *organes fédéraux* traitent des données personnelles. Dans le cas de traitements de données effectués uniquement par des personnes privées (p. ex. l'art. 12 al. 5 nLPD), aucune référence n'est faite à la protection des droits fondamentaux.

B. Termes nouveaux et élargis

1. Responsable du traitement et sous-traitant

[13] Le législateur suisse a entièrement repris les notions de « **responsable du traitement** » et de « **sous-traitant** » du RGPD. Ce sont les deux rôles essentiels sur lesquels repose la nLPD. L'ancien « maître du fichier » a été supprimé. Cependant, son rôle a été largement repris dans la définition du « responsable du traitement ». Le responsable du traitement est la personne qui, seule ou conjointement avec d'autres, « détermine les finalités et les moyens du traitement de données personnelles ». C'est la personne **qui détermine les paramètres essentiels de protection des données d'un certain traitement de données**. La logique sous-jacente est que la personne qui est *de facto* responsable de la manière dont le traitement des données est conçu devrait être la première responsable du respect de la protection des données. Il peut s'agir d'une seule personne (p. ex. une entreprise) ou de plusieurs personnes dans la mesure où elles participent – dans une mesure plus ou moins grande – à la prise de décisions concernant la finalité et les moyens du traitement. A cet égard, il n'est pas nécessaire que toutes les décisions soient prises conjointement ; une collaboration de plusieurs personnes basée sur une division du travail suffit. L'influence exercée par les différentes personnes sur la décision peut aussi varier : tant qu'il s'agit d'un même traitement de données, c'est-à-dire tant qu'il existe un lien indissociable entre les activités de traitement des différents responsables du traitement, ceux-ci sont tous responsables et considérés comme des **responsables conjoints du traitement**.

[14] A titre d'exemple, si un client confie à son prestataire de services (p. ex. son avocat) certains traitements de données dans le cadre de la prestation de services (p. ex. l'introduction d'une certaine action en justice), le client décide de la finalité (et donc de la direction) du traitement, même s'il est convenu que le prestataire de services décide de certains moyens essentiels utilisés pour exécuter le contrat (p. ex. quelles données seront traitées, comment elles seront traitées, où elles seront obtenues, à qui elles seront communiquées, combien de temps elles seront conservées), dans la mesure où il est le mieux informé à cet égard. Dans cet exemple, le client et l'avocat sont « conjointement » responsables en cas d'introduction d'une action en justice (parce que l'action est le résultat d'une collaboration et d'une répartition des tâches quant à la finalité et les moyens essentiels du traitement), alors que pour la gestion de son propre mandat, l'avocat est seul responsable (parce qu'il l'entreprend pour lui-même et l'organise lui-même, même s'il acquiert le mandat du client et agit pour le compte de celui-ci).

[15] En revanche, est considérée comme un sous-traitant, toute personne qui effectue un traitement de données **conformément à des instructions** définissant les paramètres essentiels en matière de protection des données – même si elle peut déterminer elle-même certains paramètres de traitement moins importants (p. ex. les procédés effectivement utilisés, la sélection des programmes, les mesures de sécurité des données). Un exemple classique est celui du fournisseur de services en nuage qui met ses ordinateurs et logiciels à la disposition de ses clients pour le traitement des données. Le fait qu'il offre certains services préconfigurés à ses clients ne change

pas le fait que ce sont les clients qui choisissent le moyen de traitement – de la même manière que le client d'un restaurant choisit son plat dans le menu prédéfini ou s'en va si rien ne lui convient.

[16] La délimitation entre le responsable du traitement et le sous-traitant peut s'avérer plus difficile en pratique qu'elle n'y paraît à première vue. Dans l'UE, la Cour suprême a déjà rendu plusieurs décisions sur ces **questions de délimitation**. L'auteur de cet article a déjà traité ces questions en détail dans une autre contribution et les a illustrées à la lumière de nombreux exemples tirés de la pratique[14]. Le Comité européen de la protection des données (CEPD) a récemment publié une ligne directrice pour consultation à ce sujet[15]. Certaines constellations restent toutefois encore floues. Par exemple, la question se pose de savoir si une personne qui ne détermine que les moyens essentiels du traitement, mais pas ses finalités, peut néanmoins être considérée comme responsable (conjoint) du traitement[16].

[17] Comme dans le droit actuel, toute personne qui engage un sous-traitant doit généralement s'assurer, **par le biais d'un contrat**, que le sous-traitant n'effectue le traitement des données que de la manière dont le responsable du traitement est lui-même autorisé à le faire ; si elle ne le fait pas, elle s'expose désormais à une amende (art. 9 nLPD, N 57 ss). Contrairement à l'art. 26 RGPD, la nLPD ne prévoit pas d'obligation générale de réglementer les responsabilités entre responsables conjoints du traitement dans le secteur privé. Une telle obligation peut toutefois découler de l'art. 7 al. 1 et 2 nLPD (N 43)[17].

[18] Par ailleurs, l'introduction de ces deux nouvelles notions n'a rien changé quant à la **responsabilité civile pour les violations des normes en matière de protection des données** : toute personne qui *participe* à un traitement de données portant atteinte à la personnalité d'une personne concernée peut être tenue responsable. Cela inclut également les employés et les personnes physiques autrement intégrées dans l'entreprise qui ne sont ni des sous-traitants ni des responsables du traitement, pour autant que l'atteinte à la personnalité puisse leur être imputée (la nLPD ne contient pas de disposition analogue à l'art. 29 RGPD, selon lequel les données personnelles ne peuvent être traitées que sur instruction du responsable du traitement, cf. aussi N 58).

---

14 David Rosenthal, Controller oder Processor : Die datenschutzrechtliche Gretchenfrage, in : Jusletter 17 juin 2019 ; cf. aussi David Rosenthal/Barbara Epprecht, Banken und ihre datenschutzrechtliche Verantwortlichkeit im Verkehr mit ihren Dienstleistern, in : Susanne Emmenegger (Hrsg.), Banken und Datenschutz, Bâle 2019 (http://www.rosenthal.ch/downloads/Rosenthal-Epprecht-ControllerProcessor.pdf (état au 9 mars 2021)).

15 European Data Protection Board (EDPB), Guidelines 07/2020 on the concepts of controller and processor in the GDPR (Version 1.0), 2 septembre 2020, (https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2020/guidelines-072020-concepts-controller-and-processor_en (état au 9 mars 2021)).

16 C'est le cas, selon le point de vue exprimé ici, étant donné le sens et l'objectif de la définition juridique qui est de pouvoir inclure dans la loi tous ceux qui déterminent les aspects essentiels du traitement du point de vue du droit de la protection des données (apparemment du même avis : David Vasella, Verantwortliche und Auftragsverarbeiter : Zu den Leitlinien des EDSA (Entwurf) zum « Controller » und « Processor », in : datenrecht.ch, 14 septembre 2020, ch. 1.2.1 (https ://datenrecht.ch/edsa-entwurf-von-leitlinien-zum-verantwortlichen-und-zum-auftragsverarbeiter) (état au 9 mars 2021).

17 En outre, l'art. 33 nLPD prévoit que lorsqu'un organe fédéral traite des données personnelles conjointement avec d'autres organes fédéraux, des organes cantonaux ou des personnes privées, le Conseil fédéral règle les procédures de contrôle et les responsabilités en matière de protection des données. Certaines lois cantonales sur la protection des données prévoient des règles similaires à l'art. 26 RGPD dans leur domaine compétence (p. ex. art. 5 al. 1 IDG ZH).

2. Données personnelles

[19] La notion de **données personnelles** (art. 5 let. a nLPD) a également été reprise du RGPD. Les personnes morales qui étaient auparavant protégées par la LPD ne le sont désormais plus. Elles restent toutefois protégées par l'art. 28 CC. On peut aussi supposer qu'en cas de litige concernant un traitement de données spécifique, les principes de traitement et les motifs justificatifs de la LPD s'appliqueront par analogie. Toutefois, les personnes morales ne bénéficient par exemple plus d'un droit d'accès. Pour le reste, l'acceptation de ce qui constitue des données personnelles ne change pas avec la nLPD : en Suisse, la « méthode relative », confirmée par le Tribunal fédéral, continue de s'appliquer. Elle **distingue entre l'identification objective et subjective**. Selon cette méthode, il faut se placer du point de vue de la personne qui a accès à l'information et déterminer dans chaque cas si elle (a) est en mesure d'identifier la personne physique à laquelle l'information se rapporte et (b) est également disposée à fournir les efforts nécessaires à l'identification[18].

[20] Ainsi, par exemple, les données génétiques ne constituent des données personnelles que si la personne qui y a accès a également accès à une base de données génétiques ou à une autre source d'information lui permettant d'identifier la personne concernée. Quant aux **données pseudonymisées**, c'est-à-dire les données codées ou cryptées, elles ne constituent à leur tour que des données personnelles pour les personnes qui ont accès au code permettant de rétablir la référence personnelle. Par conséquent, les données « singularisées »[19] ne constituent pas des données personnelles au sens de la nLPD, même si elles concernent une personne individuelle. Cela est également vrai en soi dans le contexte du RGPD, même si les autorités de protection des données ont affirmé à plusieurs reprises – la plupart du temps sans examen approfondi apparent – que la singularisation devait suffire pour être en présence de données personnelles. Les cookies et les adresses IP sont donc régulièrement qualifiés de données personnelles par ces autorités, bien que la CJUE ait jusqu'à présent adopté une position différente dans les deux cas[20].

3. Données personnelles sensibles

[21] Le législateur suisse n'a pas repris la définition juridique des données personnelles sensibles du RGPD. Elles sont définies de manière similaire aux « catégories particulières de données à caractère personnel » prévues à l'art. 9 RGPD, dans la mesure où leur traitement nécessite une base juridique spécifique. Toutefois, la notion suisse diffère à plusieurs égards de la notion européenne. Dans la nLPD, les données personnelles sensibles sont définies de manière plus large et comprennent, comme dans la LPD actuelle, aussi les données relatives aux poursuites ou sanctions pénales et administratives (qui sont en partie régies par l'art. 10 RGPD), les données relatives aux mesures d'aide sociale et les données relatives à la sphère intime. S'agissant de ces dernières, seules les données relatives à la vie sexuelle ou à l'orientation sexuelle sont couvertes par la notion de « catégories particulières de données à caractère personnel » du RGPD.

---

18 ATF 136 II 508, c. 3.2.

19 En d'autres termes, des données qui, comme une empreinte digitale, sont si individuelles ou « singulières », qu'elles ne peuvent se référer qu'à une seule personne, même si cette personne n'est pas encore identifiée.

20 Cf. David Rosenthal : Personendaten ohne Identifizierbarkeit ?, in : Digma décembre 2017, Numéro 4 (http ://www.rosenthal.ch/downloads/digma_2017_4_Rosenthal.pdf (état au 9 mars 2021)) ; arrêt de la CJUE du 19 octobre 2016, C-582/14 (« Breyer »), points 44-49 et arrêt de la CJUE du 1er octobre 2019, C-673/17 (« Planet49 »), point 71.

[22] Le catalogue final de l'art. 5 let. c nLPD a été élargi pour inclure les « **données génétiques** » et les « **données biométriques identifiant une personne physique de manière univoque** ». Bien que la précision « identifiant une personne physique de manière univoque » n'ait pas été ajoutée pour les données génétiques – malgré les tentatives du Conseil national – pour des raisons systématiques et téléologiques, seules les données génétiques qui répondent aux exigences des données personnelles au sens de l'art. 5 let. a nLPD sont couvertes par la nLPD. Autrement dit, le traitement des données génétiques ne relève du champ d'application de la nLPD que si ces données permettent de tirer des conclusions sur l'identité d'une personne physique. Cet élément est explicitement mentionné dans le RGPD[21]. Si les débats parlementaires suggèrent que certains parlementaires considéraient les données génétiques en elles-mêmes comme des données personnelles, ces déclarations (et d'autres) semblent être principalement l'expression d'un manque d'expertise, et non de la volonté du législateur de déclarer les données génétiques comme des données personnelles *per se*[22]. Il n'apparaît pas que le législateur suisse ait eu l'intention d'inclure des données factuelles parmi les données personnelles par le biais d'une définition juridique des données personnelles sensibles. Autre est la question de savoir dans quelle mesure il est véritablement impossible, en l'état actuel de la science, de ne pas tirer des conclusions relatives à un individu sur la base de données génétiques, dans des circonstances concrètes. L'ajout des données biométriques à l'art. 5 let. c nLPD s'avère dès lors nécessaire, sauf à considérer comme données personnelles sensibles des photos « ordinaires » de visages ou d'autres parties du corps, par exemple.

[23] La notion de « données personnelles sensibles » est encore légèrement trompeuse dans la nouvelle loi. Bien que catalogue de l'art. 5 let. c nLPD soit exhaustif, cela ne signifie pas que les données personnelles qui y sont mentionnées soient nécessairement sensibles dans des cas concrets (p. ex. les déclarations politiques d'un politicien), ni que d'autres données personnelles non mentionnées ne puissent aussi être sensibles (p. ex. des informations sur le revenu ou un profil de déplacement). Toutefois, la Suisse est toujours tenue, en vertu de la Convention du Conseil de l'Europe, de prévoir dans la LPD des règles de protection individuelle supplémentaires pour ces catégories de données personnelles. En outre, la classification des données personnelles comme « sensible » a le mérite d'offrir un indice clair quant à l'appartenance d'une donnée à la catégorie susvisée. En général, cependant, le principe de l'**application des normes en fonction du risque**, qui permet (et exige) une évaluation du cas d'espèce, continue de s'appliquer sous la nLPD : plus les données ou le traitement sont sensibles au regard du risque d'atteinte à la personnalité des personnes concernées, plus il faut prendre des précautions pour éviter qu'une telle atteinte ne se produise (cf. art. 7 et 8 nLPD).

---

21 Les données génétiques sont définies dans le RGPD comme des « données à caractère *personnel* relatives aux caractéristiques héréditaires ou acquises d'une personne physique (...) » (art. 4 al. 13 RGPD).

22 D'un point de vue systématique, la protection générale des données génétiques devrait être placée ailleurs. En effet, la définition des données personnelles sensibles indique uniquement quelles *données personnelles* sont sensibles. La classification des données génétiques comme des données personnelles sensibles suppose que la LPD mentionne clairement que les données génétiques sont des données personnelles. Aussi, il n'apparaît pas que la Suisse ait eu l'intention d'aller au-delà du champ de protection des données génétiques prévu par le RGPD. L'ajout auquel il a été renoncé ne dit également rien à cet égard : il aurait simplement indiqué que les *données personnelles* génétiques (qui sont considérées comme des données personnelles parce qu'elles sont capables d'identifier une personne) sont des données personnelles sensibles.

4. Le profilage avec et sans « risque élevé »

[24] À première vue, la Suisse semble avoir abandonné son propre concept de « profil de personnalité » qui était jusqu'ici soumis aux mêmes règles que celles applicables aux données personnelles sensibles. Le terme « **profilage** » a été introduit en lieu et place (art. 5 let. f nLPD). Contrairement à la proposition du Conseil fédéral, le Parlement a repris la définition juridique du RGPD. Le profilage commence effectivement là où se termine le profil de la personnalité : ce dernier consiste en la *collecte* de données qui *permet d'évaluer* les aspects essentiels d'une personne, alors que le profilage couvre le *processus d'évaluation* de ces aspects (c'est-à-dire ni l'entrée ni la sortie des données). Le terme « évaluation » couvre uniquement les traitements qui nécessitent une *interprétation* des données, c'est-à-dire qui **nécessitent une appréciation**, contiennent une composante subjective telle qu'une prévision. Le profilage n'est pas la détermination objective d'un fait.

[25] L'interprétation doit être **automatisée**, c'est-à-dire qu'elle ne doit pas être faite manuellement par un être humain, et elle doit se rapporter à une personne individuelle (et non à un groupe de personnes). Ainsi, par exemple, un test VIH automatisé ne constitue pas un profilage au sens de la LPD (la réponse oui/non à la simple question de savoir si des anticorps au virus sont présents sera toujours la même, peu importe la personne qui effectue le test ou l'objet avec lequel il est effectué), alors que l'analyse d'un frottis cervical chez une femme pour déterminer le risque de cancer constitue un profilage dans la mesure où elle est automatisée (car l'analyse de l'échantillon de tissu suppose une interprétation de la question de savoir s'il s'agit d'une excroissance bénigne ou maligne, qui peut aujourd'hui être faite de manière automatisée).

[26] Ce dernier exemple met aussi en évidence le risque particulier du profilage : une personne ou un aspect d'une personne est *évalué* par une machine, et non plus par un être humain. Même si l'évaluation de la machine est basée sur une commande humaine, elle se fait toujours de manière schématique. Pour qu'un processus soit considéré comme un profilage, il faut que le profilage soit la finalité ou le motif du traitement des données. Par exemple, si un marchand de vins établit des statistiques sur les types de vins achetés par ses clients afin de mieux concevoir son assortiment, il ne s'agit pas d'un profilage. Si, en revanche, à partir de la même base de données, il établit une liste de tous les acheteurs de vins espagnols dans le but de leur écrire parce qu'il pense qu'ils seront les plus à même d'être *intéressés* par une nouvelle livraison de ces vins (évaluation automatique), il s'agit d'un profilage. S'il sélectionne chaque client manuellement, ce n'est plus un profilage. En effet, la LPD ne prévoit pas de profilage manuel.

[27] S'agissant du **profilage** « **à risque élevé** » (art. 5 let. g nLPD), les Chambres n'ont pu parvenir à un accord que lors de la conférence de conciliation. Au cours des débats parlementaires, il est devenu évident pour chacun que tout profilage n'est pas nécessairement sensible, comme l'illustre l'exemple précédent du marchand de vins. Pour résoudre le problème, la notion de profil de la personnalité a été réintroduite par la petite porte : le profilage à risque élevé est celui qui conduit à une mise en relation de données permettant d'apprécier les caractéristiques essentielles de la personnalité d'un individu. Ce n'est rien d'autre que le profil de la personnalité que nous connaissons. Un exemple est celui de l'entreprise qui définit le profil de personnalité du candidat idéal pour un poste et laisse ensuite l'ordinateur déterminer quel candidat correspond le mieux à ce profil. La nouvelle réglementation est toutefois plus stricte que le droit actuel, du moins dans sa formulation : lorsqu'un ordinateur génère de manière indépendante un profil de la personnalité, il ne s'agit d'un profilage « à risque élevé » que si l'établissement de ce profil entraîne un risque élevé pour la personne concernée. Cela découle déjà de la formulation de la définition ju-

ridique (« entraînant un risque élevé [...] *parce qu'il* conduit à un appariement de données [...] »). Le risque réel d'atteinte aux droits de la personnalité dépend des mesures de protection prises dans le cas particulier. Le point de vue alternatif – parfois défendu au Parlement – selon lequel l'existence d'un profil de la personnalité entraîne *per se* un risque élevé, ne semble pas justifié et entraînerait des problèmes conséquents[23] (cf. à ce sujet, les commentaires sur l'analyse d'impact relative à la protection des données, N 148 ss). Inversement, le profilage peut entraîner un risque élevé même sans profil de la personnalité. Partant, il semble plus logique de procéder à une interprétation indépendante de la définition juridique. L'ajout du concept de « profilage à risque élevé » ne compense dès lors que partiellement la suppression du « profil de la personnalité » dans la mesure où il est désormais nécessaire d'être à tout le moins en présence d'une évaluation automatisée. Lorsqu'il n'est fait référence qu'au « profilage », ce qui est le cas notamment de certaines dispositions importantes pour les organes fédéraux[24], la nLPD a été renforcée car elle couvre désormais davantage que le droit actuel, à savoir toutes les mises en relation de données qui permettent d'apprécier les caractéristiques (même non essentielles) de la personnalité d'un individu.

[28] Le profilage a fait l'objet de nombreux débats au Parlement et parmi le grand public. La **pertinence juridique de cette notion** est toutefois limitée. Hormis les exigences relatives à la validité du consentement (N 30 ss) et à la justification de l'évaluation de la solvabilité de la personne concernée (N 42), le profilage ne figure pas dans les dispositions de la LPD applicables au secteur privé. En effet, le Parlement a supprimé le profilage des dispositions relatives aux décisions individuelles automatisées (N 106 ss) et à l'analyse d'impact relative à la protection des données (N 148 ss). Autrement dit, le Parlement a débattu d'une définition juridique sans conséquences juridiques réelles, du moins en ce qui concerne les personnes privées responsables du traitement. Un droit d'objection spécifique au profilage – que la gauche voulait introduire – n'a finalement pas été adopté. Le profilage n'est pas davantage limité par la LPD que tout autre traitement de données. L'approche fondée sur le risque s'applique également ici, c'est-à-dire qu'il faut vérifier, par exemple, si le profilage est proportionné et si l'évaluation d'une personne concernée ne devrait pas plutôt être laissée à une personne qui procède à une évaluation au cas par cas. Il faut aussi vérifier que les principes de finalité et de transparence, applicables à tout traitement de données, sont respectés. En pratique, de nombreux profilages seront absolument inoffensifs, et même bien plus inoffensifs qu'un profil de la personnalité. Il est donc regrettable que les organes fédéraux doivent désormais disposer d'une base juridique formelle pour tout profilage (art. 34 al. 2 let. b nLPD). Soulignons enfin que le profilage n'est pas soumis à une exigence de consentement sous la nLPD, même dans le cas d'un profilage à risque élevé[25].

---

23 Une fiction du risque élevé ignorerait complètement les effets *réels* de l'utilisation d'un profil de la personnalité. Toute utilisation d'un profil de la personnalité serait *per se* classée comme étant à risque élevé et devrait toujours fait l'objet d'une consultation préalable du PFPDT (art. 23 nLPD). Rien n'indique que le législateur ait voulu une telle protection de la personnalité, qui va bien au-delà du profilage et du droit actuel, par le biais d'une définition juridique détournée du « profilage à risque élevé ». Le profilage à risque élevé n'est, après tout, qu'un compromis trouvé *in extremis* dans le cadre des débats parlementaires sur l'étendue de la protection des personnes concernées face au profilage. Les Conseils se sont uniquement concentrés sur la question du consentement et de l'évaluation du crédit. Le « risque élevé » selon la définition juridique devrait donc être différent de celui énoncé à l'art. 23 nLPD.

24 Par exemple, art. 34 nLPD.

25 Dans ce sens, cf. aussi David Vasella, Neues DSG : kein grundsätzliches Einwilligungserfordernis beim Profiling, auch nicht bei hohem Risiko, in : datenrecht.ch, 25 septembre 2020 (https ://datenrecht.ch/neues-dsg-kein-grundsaetzliches-einwilligungserfordernis-beim-profiling-auch-nicht-bei-hohem-risiko/ (état au 9 mars 2021)).

5. Violation de la sécurité des données

[29] Voir les explications sous N 160.

C. Consentement

[30] La définition juridique du consentement n'a, à juste titre, pas changé en substance. Le Parlement a supprimé la précision proposée par le Conseil fédéral selon laquelle le consentement devrait être donné sans ambiguïté. Il est donc clair qu'**aucune autre norme ne s'applique au consentement** dans le droit de la protection des données, comme c'était le cas auparavant et comme c'est par ailleurs le cas en droit suisse en ce qui concerne les déclarations de volonté. L'unité de la matière juridique est ainsi préservée. En outre, il était déjà clair que plus le risque pour la personne concernée par un traitement données est élevé, plus les exigences en matière de validité du consentement sont élevées. Contrairement à ce qui est prévu dans le RGPD[26], les cases d'un formulaire électronique peuvent en principe toujours être pré-cochées[27] car, en droit suisse, la validité du consentement ne nécessite pas d'information sur le droit de retirer son consentement et il n'existe pas d'interdiction de couplage au sens de l'art. 7 al. 4 RGPD[28] (cf. aussi N 51). Le consentement des enfants est également régi de manière moins rigide en droit suisse qu'en vertu de l'art. 8 RGPD[29].

[31] L'art. 6 al. 6 et 7 nLPD, qui ne fait que définir les conditions dans lesquelles le consentement est valable dans le cadre de la LPD, n'a pas non plus été modifié. Cet article n'indique pas si le consentement est en principe requis, ni dans quels cas il est nécessaire[30]. Les cas dans lesquels le consentement est requis ou sert de motif justificatif sont énoncés ailleurs dans la nLPD, à

---

26 Cf. arrêt de la CJUE du 1er octobre 2019, C-673/17 (« Planet49 »), point 62, citant le considérant 32 RGPD lequel indique que les cases cochées par défaut ne constituent pas un consentement de la personne concernée.

27 L'élément décisif est que la case cochée devienne partie intégrante de la déclaration de volonté de la personne concernée lorsqu'elle confirme le formulaire, ce qui est généralement le cas si la personne concernée peut l'identifier comme telle avant la confirmation. Cela s'applique également dans le cas d'un consentement explicite. Par exemple, lorsqu'une personne saisit son adresse sur un formulaire d'inscription et laisse la case qui signale son consentement au traitement de données décrit dans le formulaire préalablement cochée, puis confirme, en appuyant sur un bouton, l'ensemble du formulaire comme étant le contenu de sa déclaration de volonté, démontre, par son comportement actif (appuyer sur le bouton), qu'elle consent explicitement au traitement des données envisagé (N 32). Si le fait de cocher activement la case était également demandé, alors il faudrait deux déclarations de volonté pour qu'un même consentement soit valable. Même avec un formulaire papier, personne en droit suisse n'envisagerait de demander qu'une case soit activement cochée pour qu'une déclaration de consentement reproduite sur le formulaire soit réputée avoir été explicitement donnée lors de la signature du formulaire. Il en serait tout au plus différent si la déclaration de consentement était « cachée » sur le formulaire de telle manière à ce que l'on ne pourrait pas s'attendre à ce que l'utilisateur en prenne connaissance – et, même dans ce cas, la question se pose de savoir si, comme dans le cas des conditions générales soumises aux réserves des clauses insolites, elle ne devrait pas logiquement s'appliquer après tout.

28 En Suisse également, la conclusion d'un accord ne peut pas être arbitrairement subordonnée à la condition que le consentement à un certain traitement de données soit donné, car un tel lien pourrait affecter le caractère volontaire du consentement. A cet égard, notons que les obstacles en droit suisse sont beaucoup plus importants que ceux en vertu du RGPD : le consentement est réputé donné volontairement lorsqu'il est directement lié aux données pour le traitement desquelles il est obtenu et qu'il n'y a pas de contrainte inadmissible pour l'obtenir (cf. arrêt du Tribunal administratif fédéral du 19 mars 2019, A-3548/2018 « Helsana+ », c. 4.7).

29 Pour les mineurs, la validité des consentements en vertu de la LPD est généralement régie par l'art. 19 CC. Cette disposition prévoit que les mineurs qui ont la capacité de discernement peuvent prendre leurs propres décisions. La capacité de discernement est généralement présumée dès l'âge de 13 ans.

30 Dans ce sens, cf. aussi David Vasella, Neues DSG : kein grundsätzliches Einwilligungserfordernis beim Profiling, auch nicht bei hohem Risiko, in : datenrecht.ch, 25 septembre 2020 (https ://datenrecht.ch/neues-dsg-kein-grundsaetzliches-einwilligungserfordernis-beim-profiling-auch-nicht-bei-hohem-risiko/ (état 9 mars 2021)).

savoir aux art. 17 al. 1 let. a nLPD (exportation de données), 21 al. 3 let. b nLPD (décisions individuelles automatisées), 25 al. 3 nLPD (droit d'accès aux données personnelles sur la santé), 31 al. 1 nLPD (motifs justificatifs), 34 al. 4 let. b nLPD (traitement de données sans base légale par des organes fédéraux) et 36 al. 2 let. b nLPD (communication de données personnelles par des organes fédéraux). En pratique, il subsiste une certaine incertitude s'agissant du moment où le consentement doit être obtenu. Toutefois, la LPD est claire à cet égard : il n'y a **pas de changement par rapport à la situation juridique actuelle**. Le législateur n'avait pas non plus l'intention de modifier la pratique actuelle. Cela serait également contraire au concept (N 40). Les propositions visant à établir une obligation de consentement de la personne concernée pour certains traitements de données ont été rejetées lors des débats parlementaires[31].

[32] Il n'est pas non plus nécessaire d'obtenir de consentement en vertu de l'art. 6 al. 7 nLPD, qui traite du traitement de données sensibles et du profilage avec ou sans risque élevé (selon qu'un organe fédéral est impliqué ou non). Là encore, la disposition prévoit simplement que, si le consentement est requis dans de tels cas, il doit être exprès. Une certaine confusion subsiste quant à la signification du terme « **exprès** ». Cela ne signifie pas que le consentement doit être donné par écrit. Le terme « exprès » est le contraire d'« implicite » et c'est ainsi qu'il doit être compris : le consentement est exprès s'il y a (i) un comportement actif ou un comportement qui a été convenu comme affirmatif (p. ex. au moyen d'une clause dans les conditions générales qui stipule que le silence suite à une modification des conditions générales vaut consentement) et (ii) la portée de ce comportement affirmatif est directement liée au traitement des données en question[32]. Par contre, le consentement est implicite si le comportement affirmatif n'est pas lié au traitement des données, mais uniquement à l'action aboutissant au traitement des données. Ainsi, par exemple, une personne qui consent à recevoir de la publicité personnalisée ne consent pas en même temps expressément à la mise en œuvre du profilage à risque élevé sous-jacent à cette publicité, que le consentement à recevoir la publicité ait été exprès ou non. Le traitement des données doit donc être *mentionné explicitement*.

D. Principes du traitement des données

1. Les principes de traitement

[33] Les principes de traitement se trouvent désormais à l'art. 6 nLPD. Ils ont été légèrement révisés d'un point de vue linguistique, **mais correspondent en substance au droit actuel**. Du moins, c'est ainsi que le message du Conseil fédéral le conçoit[33] et, au fond, cela a du sens. En pratique, cela signifie que les traitements de données autorisés en vertu de la LPD le resteront en principe après l'entrée en vigueur de la nLPD. Les modifications apportées à l'art. 6 nLPD sont principalement liées à un alignement linguistique sur le RGPD. D'un point de vue dogmatique, cependant, le législateur s'est montré confus : le principe de l'exactitude (matérielle) des données pêche par sa formulation trop longue, le principe de proportionnalité apparaît désormais deux

31 CE, BO 2019, p. 1246 ss, session d'hiver 2019, 18 décembre 2019.

32 Cf. David Rosenthal, Der Vorentwurf für ein neues Datenschutzgesetz : Was er bedeutet, in : Jusletter 20 février 2017, N 31 ss.

33 FF 2017 6644 ss.

fois (art. 5 al. 2 et 4 nLPD) et le principe de transparence, malgré son importance en tant que règle explicite, a été supprimé du libellé de l'art. 6 nLPD sans que cela eût été nécessaire.

[34] Selon l'art. 6 nLPD, tout traitement de données personnelles doit être **licite** (al. 1), c'est-à-dire qu'il ne doit pas enfreindre une autre norme du droit suisse visant directement ou indirectement à protéger la personnalité[34], à l'instar du droit à l'image. Le traitement doit être effectué de bonne foi et être **proportionné** à tous égards (al. 2). Le principe de proportionnalité signifie que le traitement doit être nécessaire, apte à produire les résultats escomptés et proportionné au sens étroit du terme, c'est-à-dire raisonnable du point de vue de la personne concernée. La nouvelle exigence énoncée à l'al. 4, selon laquelle les données doivent être détruites ou anonymisées dès qu'elles ne sont plus nécessaires au regard des finalités du traitement, ne fait que répéter ce qui est déjà prévu à l'al. 2. Le terme « détruit » ne doit pas être pris au pied de la lettre : bien entendu, l'effacement des données conformément aux exigences de la protection des données suffit[35] ; il n'est pas nécessaire de détruire les données, car la destruction implique la destruction du support de données. Il suffit de s'assurer qu'il n'y a plus de données personnelles, raison pour laquelle l'al. 4 mentionne également l'anonymisation des données. Même la pseudonymisation des données peut être suffisante si la personne n'a plus besoin des données et ne possède plus la clé pour les décrypter (et les personnes non autorisées non plus). L'al. 4 ne décrit qu'un seul aspect de la proportionnalité ; les autres aspects, tels que le principe de minimisation des données, découlent de l'al. 2, comme c'est déjà le cas dans le droit actuel.

[35] Le **principe de finalité** de l'art. 6 al. 3 nLPD a été reformulé. En termes de contenu, le principe reste le même, avec une restriction (N 36). Comme dans la loi actuelle, les données personnelles ne peuvent être traitées qu'à des fins reconnaissables pour la personne concernée au moment de la collecte des données. C'est en principe (toujours) le cas lorsque la personne concernée a été informée préalablement à la collecte, lorsque le traitement est prévu par le droit suisse ou lorsqu'il ressort clairement des circonstances[36]. Le principe de transparence doit également être pris en compte – ce qui n'est qu'à moitié vrai : bien que l'art. 6 al. 3 nLPD exige que la collecte des données personnelles soit reconnaissable en tant que telle pour la personne concernée (pas de collecte secrète) et que les finalités du traitement lui soient communiquées, il n'est pas nécessaire que les autres paramètres du traitement soient reconnaissables. A teneur du libellé de l'art. 6 al. 3 nLPD, les devoirs d'information sont moins complets que dans la formulation actuelle de l'art. 4 al. 4 LPD sur le **principe de reconnaissabilité**. Il convient, sur le plan dogmatique, de revenir sur le principe du traitement de bonne foi au sens de l'art. 6 al. 2 nLPD qui – avant même l'introduction du principe de reconnaissabilité en 2008 – exigeait que le traitement des données soit effectué de manière transparente. En d'autres termes, l'art. 6 al. 3 nLPD exige que la collecte des données et les finalités du traitement soient reconnaissables pour la personne concernée, alors que l'al. 2 dispose que d'autres paramètres importants du traitement des données doivent également être reconnaissables pour la personne concernée selon les circonstances, au moins dans la mesure où ils sont susceptibles de présenter un intérêt particulier pour elle. Un intérêt particulier peut exister, par exemple, dans le fait de savoir quelles données sont traitées (p. ex. la possibilité

34 Arrêt du TAF du 19 mars 2019, A-3548/2018, c. 5.4.4.

35 Sur la question de savoir à partir de quel moment les données sont supprimées, cf. David Rosenthal, Löschen und doch nicht löschen, in : Digma, décembre 2019, Numéro 4 (http://www.rosenthal.ch/downloads/digma_2019_4_Rosenthal.pdf (état au 9 mars 2021)).

36 FF 2017 6644.

de reconnaître l'angle de vue d'une caméra de sécurité dans le bâtiment) ou à qui les données sont communiquées (p. ex. les autorités). L'art. 19 nLPD prévoit aussi un devoir d'informer. Toutefois, cette disposition n'a pas pour but de fournir aux personnes concernées, sur demande, des informations supplémentaires concernant le traitement de leurs données. Le devoir d'informer prévu à l'art. 19 nLPD est de nature publique, tandis que le principe de traitement de l'art. 6 nLPD est une concrétisation de l'art. 28 CC. Pour illustrer ces dispositions, prenons l'exemple des denrées alimentaires : le consommateur doit pouvoir reconnaître immédiatement de quoi il s'agit (confiture de fraises), tandis que les petits caractères sur l'étiquette révèlent la composition détaillée. La première information (confiture de fraise) correspond à la mise en œuvre du principe de transparence au sens de l'art. 6 nLPD et la seconde à la mise en œuvre du devoir d'informer au sens de l'art. 19 nLPD.

[36] La notion de « **compatibilité** » **avec la finalité initiale du traitement** est une nouveauté, introduite à l'art. 6 al. 3 nLPD. Le RGPD connaît déjà cette notion, qui est développée à son art. 6 al. 4. Cette notion de « compatibilité » élargit le cercle des finalités autorisées au-delà de celles qui sont reconnaissables pour la personne concernée. Par exemple, si une boutique en ligne collecte des données sur ses clients pour le traitement des commandes, cette finalité est reconnaissable pour ses clients et donc couvert par le principe (étroit) de finalité. En revanche, si la même boutique en ligne commence à analyser ces données à des fins de lutte contre la fraude, elle n'utilise plus les données pour la finalité pour laquelle elles ont été collectées. Auparavant, ce cas constituait une violation du principe de finalité, qui devait être justifiée conformément à l'art. 13 LPD. Ce n'est plus le cas aujourd'hui : la finalité secondaire est dans ce cas « compatible » avec la finalité primaire, de sorte qu'elle est également couverte. En revanche, si la boutique établit, à partir de ces données, des profils de ses clients avec leurs habitudes de consommation afin de pouvoir leur proposer des offres publicitaires personnalisées, cela n'est pas compatible avec la finalité (primaire) du traitement[37]. Si la boutique en ligne souhaite le faire, elle n'a pas besoin de requérir le consentement de ses clients, mais devra les informer à l'avance, par le biais de sa déclaration de protection des données, qu'elle utilisera également leurs données à des fins de publicité personnalisée (et non de prévention de la fraude), et pas seulement pour le traitement des commandes – à moins que ces fins ne soient déjà reconnaissables pour les clients dans le cas d'espèce. Il s'agit alors d'une finalité supplémentaire, officiellement communiquée à la personne concernée, de sorte qu'elle peut s'écarter de la finalité initiale (exécution du contrat). Un autre exemple classique de traitement des données généralement compatible avec la finalité initiale est la pseudonymisation ou l'**anonymisation des données afin de les utiliser à d'autres fins** (p. ex. pour les communiquer à un tiers pour lequel elles ne sont plus des données personnelles). Jusqu'à présent, cela constituait également à proprement parler une violation du principe de finalité, sauf si le responsable du traitement lui-même ne disposait plus d'une copie des données personnelles (auquel cas l'anonymisation équivalait à l'effacement des données et, par conséquent, la LPD n'était plus applicable). Toutefois, la nLPD ne définit pas réellement quand une finalité secondaire est « compatible » avec la finalité initiale et – contrairement au RGPD – ne fournit aucune indication à cet égard[38]. Selon le message du Conseil fédéral, toute finalité secondaire qui serait considérée comme « inattendu[e], inapproprié[e] ou contestable »[39] au regard de la finalité

37 Cf. FF 2017 6645 (exemple similaire).

38 Cf. art. 6 al. 4 RGPD.

39 FF 2017 6645.

initiale, n'est pas compatible avec la finalité initiale. Le Conseil fédéral cite, à titre d'exemples, la collecte et l'utilisation d'adresses e-mails transmises sur Internet par la personne concernée pour l'envoi de publicité non sollicitée, et l'utilisation à des fins publicitaires des adresses obtenues dans le cadre de la récolte de signature pour une initiative populaire[40]. Le premier exemple (collecte d'adresses emails sur Internet) est toutefois déplacé, car dans le cas de données publiées par une personne elle-même, une autre disposition s'applique dans tous les cas[41]. Par conséquent, en pratique le critère de « compatibilité » ne changera guère dans la plupart des cas, du moins pour les personnes privées responsable du traitement. D'un point de vue dogmatique, le problème se posera surtout pour les traitements de données secondaires.

[37] Les longs développements sur l'**exactitude des données** à l'art. 6 al. 5 nLPD ne modifient pas non plus le principe existant selon lequel les données doivent être exactes « uniquement » au regard de leur finalité de traitement. Ainsi, par exemple, une personne qui reçoit de la correspondance commerciale contenant de fausses accusations à l'encontre d'un individu n'est pas tenue de la détruire si elle la reconnaît comme fausse, car sa conservation ne sert pas à documenter l'exactitude du contenu, mais seulement le fait que des accusations ont été formulées. L'al. 5 précise désormais que le responsable du traitement doit agir de sa propre initiative s'il constate que des données personnelles qu'il conserve sont inexactes, c'est-à-dire qu'il ne doit pas ou ne peut pas attendre que la personne concernée se plaigne. Toutefois, le Parlement a également précisé, en ajoutant la deuxième phrase à l'al. 5 au cours des délibérations, que des mesures correctives ou – si de telles mesures ne sont pas possibles – l'effacement des données ne sont nécessaires que lorsqu'elles paraissent proportionnées. Par exemple, toute personne qui constate, lors de l'envoi de cartes de Noël, que certaines lettres sont retournées faute d'avoir pu être délivrée à leurs destinataires peut, si elle le souhaite, conserver ces adresses postales dans sa liste de diffusion, car les adresses incorrectes ne causent aucun dommage pour les personnes concernées. Soulignons enfin que le droit de rectification n'est plus situé, à juste titre, dans les principes de traitement, mais dans une disposition distincte, à savoir à l'art. 32 al. 1 nLPD (cf. N 137 ss).

2. Autres principes de traitement, atteintes à la personnalité

[38] Outre le principe de la sécurité des données énoncé à l'art. 8 nLPD (N 53), l'art. 30 nLPD contient également deux autres principes (auparavant énoncés à l'art. 12 LPD) qui, par leur nature, sont également des principes de traitement :

a. Les **données sensibles ne peuvent pas être communiquées à des tiers** (al. 2 let. c). Le terme « tiers » désigne les responsables indépendants du traitement, c'est-à-dire les personnes qui ne sont pas des sous-traitants ou des responsables conjoints du traitement dans le cadre d'un traitement commun de données. Ce principe (qui existe déjà dans la LPD) ne peut pas être directement dérivé de l'art. 28 CC et des principes généraux de la protection de la personnalité. Il s'agit d'une décision délibérée du législateur en application des exigences du droit européen. Le principe est moins étendu que dans la LPD car, auparavant, il couvrait également la communication des profils de la personnalité à des tiers. Ce n'est plus le cas aujourd'hui, car la notion suisse de « profil de la personnalité » a été abandonnée sans être

40 FF 2017 6645.

41 Art. 30 al. 3 nLPD.

remplacée. Le fait que le terme ait été réintroduit indirectement par le biais du profilage à risque élevé n'y change rien. Sur ce point, la nLPD va donc moins loin que la LPD.

b. Les données personnelles ne peuvent être traitées **contre la manifestation expresse de la volonté de la personne concernée**. Ce principe est particulièrement central dans le droit suisse de la protection des données. Contrairement au RGPD, la nLPD (comme la LPD) ne requiert pas de base juridique pour le traitement des données personnelles. Elle repose sur le **principe de l'**« **opt-out** » : si la personne concernée ne souhaite pas que des données personnelles soient traitées, elle doit s'opposer au traitement en tout ou en partie. Elle n'a pas besoin d'un motif pour cela ; un tel motif ne joue de rôle qu'au niveau de la justification (cf. N 40 ss). Inversement, cela signifie que si une personne privée (c'est-à-dire qui n'est pas une autorité) souhaite traiter des données personnelles dans un but précis et s'engage à respecter les principes de traitement, elle pourra le faire aussi longtemps que la personne concernée ne s'y oppose pas. Il n'est *pas* nécessaire d'obtenir le consentement pour traiter des données personnelles, même s'il s'agit de données sensibles, bien que le PFPDT ait parfois soutenu le contraire. Seule la *communication* à des tiers doit être justifiée, mais pas le traitement lui-même. Le principe de l'« opt-out » s'applique aussi au profilage – du moins tant qu'il est proportionné et, en particulier, que l'on peut raisonnablement s'attendre à ce que la personne concernée l'accepte. Les avis divergent quant à la mesure dans laquelle on peut s'attendre à ce que la personne concernée accepte le profilage de ses données. Si le profilage n'implique pas un risque élevé, aucune justification ne sera en principe nécessaire. L'art. 30 al. 2 let. b nLPD correspond aussi à la mise en œuvre suisse du « **droit à l'oubli** » : la personne concernée peut s'opposer à tout aspect du traitement, y compris à la conservation ultérieure de ses données. Elle peut donc – indirectement – demander l'effacement de ses données (cf. également N 137). Cet argument a également été utilisé au Parlement pour rejeter le droit d'opposition spécial proposé pour le profilage à risque élevé : le principe de l'« opt-out » permet déjà à une personne concernée de s'opposer à un tel profilage. Aujourd'hui, de nombreuses entreprises accordent déjà explicitement à leurs clients la possibilité de s'opposer au profilage à des fins de marketing. Cela devrait devenir la norme dans les années à venir.

[39] Si ces deux principes de l'art. 30 nLPD ou les principes de traitement des art. 6 et 8 nLPD sont violés par un sous-traitant privé, alors conformément à l'art. 30 al. 2 nLPD et comme auparavant, **il y a atteinte à la personnalité de la personne concernée *per se*** et le traitement des données est inadmissible, sauf motif justificatif. Cette règle ne s'applique toutefois pas aux organes fédéraux. Là, ce n'est pas le système de justification qui s'applique, mais le principe de légalité. Ainsi, toute personne qui traite des données personnelles en tant qu'organe fédéral doit, d'une part, respecter les principes de traitement – sauf si la loi en dispose autrement – et, d'autre part, disposer d'une base légale pour traiter les données (art. 34 al. 1 nLPD). Dans certains cas, la base légale doit même être prévue dans une loi au sens formel, par exemple lorsqu'il s'agit d'un profilage ou d'un traitement de données sensibles (art. 34 al. 2 nLPD). Ce n'est que dans des cas exceptionnels qu'un organe fédéral peut traiter des données sans base légale, par exemple lorsque la personne concernée a consenti au traitement dans le cas d'espèce ou a rendu ses données personnelles accessibles à tout un chacun et ne s'est pas expressément opposée au traitement (art. 34 al. 4 nLPD).

3. Motifs justificatifs

[40] Les motifs justificatifs sur lesquels une personne privée traitant des données personnelles peut s'appuyer sont restés largement inchangés. Comme auparavant, ces motifs sont le consentement de la personne concernée, une base légale en droit suisse et un intérêt privé ou public prépondérant (art. 31 al. 1 nLPD) – bien que, dans la pratique, ce soit l'**intérêt privé prépondérant** qui soulève le plus de questions. C'est pourquoi l'art. 31 al. 2 nLPD énumère un certain nombre de cas dans lesquels un intérêt privé prépondérant du responsable du traitement peut généralement être présumé. La liste n'est toutefois pas exhaustive. Elle n'est pas non plus identique à la liste de l'art. 17 nLPD, qui énumère les cas dans lesquels l'exportation de données vers des pays ne disposant pas d'une protection des données adéquate peut être justifiée. Les cas énumérés à l'art. 17 nLPD fournissent néanmoins des indications supplémentaires sur les cas dans lesquels un intérêt prépondérant peut (également) exister[42]. Il ressort déjà clairement de la liste de l'art. 31 nLPD que les intérêts économiques peuvent également être invoqués, ce que la jurisprudence a confirmé il y a des années. En outre, les intérêts de *chaque personne* à effectuer le traitement peuvent être invoqués pour faire valoir un intérêt privé prépondérant.

[41] L'intérêt à effectuer le traitement des données doit être mis en balance avec l'intérêt de la personne concernée à *s'opposer* au traitement, c'est-à-dire l'intérêt à ce que le traitement des données ne soit pas effectué de la manière prévue en raison de ses conséquences pour la personne concernée. À ce stade, il peut être important de savoir pourquoi une personne concernée s'oppose au traitement et souhaite par exemple que ses données soient supprimées. En définitive, la pesée des intérêts implique souvent la recherche d'un **compromis compatible avec la protection des données**. Un tel droit à l'effacement n'est donc jamais absolu, même si, dans certains cas, il y aura peu de raisons de s'opposer à l'effacement (p. ex. certaines utilisations de données à des fins de marketing). Bien qu'il existe une jurisprudence selon laquelle un intérêt privé prépondérant ne doit pas être admis à la légère, la jurisprudence indique aussi que la pesée des intérêts – même par les juges – est généralement une décision purement intuitive fondée sur le « bien et le mal » dans un cas concret. Conceptuellement, il convient de peser les intérêts en jeu, sans négliger les intérêts de la personne concernée, car aucune des méthodes d'interprétation ne justifierait une telle partialité.

[42] Quatre modifications ont été apportées à la liste exemplative des motifs justificatifs de l'art. 31 al. 2 nLPD :

a. La modification la plus importante concerne la justification du **traitement des données à des fins ne se rapportant pas à des personnes** (let. e). Il s'agit de cas dans lesquels des données personnelles sont traitées sans rapport avec la personne concernée. Il est donc question de traitements de données à des fins non personnelles. Un exemple classique est le traite-

42 En pratique, un tel intérêt prépondérant peut être pertinent, par exemple, dans le cadre de procédures judiciaires et administratives étrangères, car dans ces cas, les données personnelles doivent souvent être communiquées sans que la personne concernée en soit préalablement informée. Dans ces cas, il est admis que la communication des données puisse être dans l'intérêt prépondérant du responsable du traitement lorsque des mesures ont été prises pour protéger les personnes concernées (cf. art. 17 al. 1 let. c ch. 2 nLPD). Un autre exemple tiré de l'art. 17 nLPD et qui peut être appliqué par analogie concerne la communication des données aux fins de l'exécution d'un contrat aux termes duquel le traitement des données ne porte pas sur les données du partenaire contractuel, mais sur celles d'une autre personne dans l'intérêt de laquelle le contrat est exécuté (par exemple, le bénéficiaire d'un cadeau) et qui, à proprement parler, n'est pas couverte par l'art. 31 al. 2 let. a nLPD, alors que l'art. 17 al. 1 let. b nLPD couvre ce cas.

ment de données à des fins statistiques. La recherche clinique basée sur les données des patients a souvent joué un rôle dans les délibérations ; l'industrie pharmaceutique, en particulier, a fait pression pour que la disposition soit adaptée par rapport au projet du Conseil fédéral. Ce n'était pas nécessaire dans la mesure où, dans le domaine de la recherche sur l'être humain et – spécifiquement pour l'utilisation secondaire des données personnelles liées à la santé –, la Loi fédérale relative à la recherche sur l'être humain (LRH)[43] prime sur la LPD en tant que *lex specialis*.

Le traitement des données à des fins non personnelles peut également être justifié sans le consentement de la personne concernée au sens de l'art. 31 al. 2 let. e nLPD, s'il est garanti que les données personnelles sont rendues anonymes *dès que possible* ou s'il est garanti d'une autre manière que l'identification des personnes concernées est empêchée. L'identification peut être empêchée, par exemple, en utilisant des codes qui ne sont accessibles qu'à un cercle limité de personnes, au lieu de vrais noms (pseudonymisation). Cette condition, selon laquelle l'identité de la personne à l'origine des données ne doit pas être reconnaissable, est nouvelle par rapport à la situation juridique actuelle. Selon la LPD actuelle, le traitement des données à des fins non personnelles est en principe toujours justifié si les données sont publiées – tout au plus – de manière anonyme. La deuxième condition, selon laquelle les *données sensibles* ne peuvent être communiquées à des tiers que si elles ont été *préalablement* rendues anonymes ou pseudonymisées, est également nouvelle. Toutefois, dans la mesure où cela n'est pas toujours possible (p. ex. parce que les partenaires de recherche sont considérés comme des responsables indépendants du traitement et donc comme des tiers), il est aussi suffisant d'obliger les tiers à veiller à que les données personnelles ne soient pas traitées à des fins personnelles. Enfin, la troisième condition n'est pas nouvelle : les résultats du traitement, une fois publiée, ne doivent plus contenir de données personnelles ; en d'autres termes, les travaux de recherche publiés ne doivent pas contenir de données permettant d'identifier les personnes concernées. Si l'identification des personnes concernées est possible, leur consentement sera généralement requis. Cette justification est particulièrement importante pour les utilisations secondaires de données personnelles, pour autant que les données personnelles ne soient pas traitées à l'égard de la personne concernée. Par exemple, si une entreprise souhaite savoir pourquoi ses clients achètent certains produits plutôt que d'autres, cette justification s'applique. En revanche, si elle souhaite s'adresser spécifiquement aux clients qui pourraient être enclins à acheter certains produits, elle ne s'applique pas.

b. Le motif justificatif du traitement des données aux fins d'**évaluer la solvabilité de la personne concernée** (let. c) a été le plus discuté dans le cadre de la révision, car trois nouvelles restrictions ont été introduites pour garantir la validité de la justification. *Premièrement*, seules les données des personnes majeures peuvent être traitées, c'est-à-dire que les agences de crédit ne peuvent plus identifier les mineurs en tant que tels dans leurs bases de données. *Deuxièmement*, les données sur lesquelles se fondent les rapports de solvabilité des agences de crédit ne peuvent plus remonter à plus de dix ans. Auparavant, il n'y avait pas de limite fixe, mais (à juste titre) seul le principe de proportionnalité s'appliquait, ce qui permettait

43 Loi fédérale relative à la recherche sur l'être humain (Loi relative à la recherche sur l'être humain, LRH) du 30 septembre 2011, RS 810.30.

de retenir une durée maximale différente selon le type d'information[44]. À première vue, la portée de la nouvelle restriction semble plus limitée qu'elle n'y paraît. La limite temporelle ne concerne que les faits qui remontent à plus de dix ans. Le fait qu'une personne siège au conseil d'administration d'une société ou qu'il existe encore un acte de défaut de biens non prescrit à l'encontre de cette personne est actuel, même si la personne occupe cette fonction depuis 30 ans ou si l'acte de défaut de biens a été émis il y a 15 ans. Toutefois, l'information selon laquelle une personne a été déclarée en faillite ne peut plus être traitées après dix ans ; auparavant, cette information était conservée pendant vingt ans au maximum. L'agence de crédit devra également vérifier, au plus tard après dix ans, si les facteurs de solvabilité enregistrés auprès d'elle existent toujours (comme dans l'exemple de l'acte de défaut de bien ou de l'administrateur). *Troisièmement*, les rapports de solvabilité ne doivent pas être basés sur un profilage à risque élevé ou sur des données personnelles sensibles – l'établissement des rapports eux-mêmes peut être un profilage, c'est-à-dire qu'ils peuvent encore afficher un feu vert, jaune ou rouge, par exemple, en fonction des données relatives à la personne concernée. La *quatrième* condition, selon laquelle les rapports de solvabilité ne peuvent être accessibles qu'aux personnes souhaitant conclure ou exécuter un contrat avec la personne concernée, reste inchangée. Elle s'appliquait déjà dans le cadre de la LPD.

Deux autres points sont souvent négligés dans la pratique : tout d'abord, le motif justificatif n'est pertinent que pour les responsables du traitement qui sont chargés de traiter des informations sur la solvabilité de tiers, c'est-à-dire les agences de crédit et les autres organismes similaires. Leurs clients (c'est-à-dire les entreprises qui utilisent ces informations pour décider d'accorder ou non un crédit à un consommateur) ne sont pas limités, car ils peuvent invoquer le motif justificatif de la conclusion du contrat (art. 31 al. 2 let. a nLPD). En outre, le motif justificatif n'est pertinent que s'il existe une atteinte à la personnalité de la personne concernée. A cet égard, on peut argumenter avec de bonnes raisons que, compte tenu du principe de transparence, il n'y a atteinte à la personnalité que lorsqu'une personne enregistrée par une agence de crédit s'oppose au traitement de ses données. Cette argumentation s'applique *a fortiori* si la personne concernée a rendu les données accessibles à tout un chacun, car l'art. 30 al. 3 nLPD est alors applicable. Selon ce raisonnement, les données de plus de dix ans peuvent être traitées dans l'attente d'une telle opposition, sous réserve que le traitement soit proportionné et que la personne concernée ne l'ait pas contesté. Par conséquent, une agence de crédit n'est pas obligée de supprimer une personne de sa base de données simplement parce qu'elle n'a pas eu de ses nouvelles depuis dix ans.

c. Une troisième modification concerne l'ajout du motif justificatif du traitement des **données personnelles de concurrents** (let. b), qui ne s'oppose plus à l'échange de données au sein d'un groupe de sociétés. Comme les données des personnes morales ne sont plus couvertes dans la nLPD, cette modification jouera un rôle secondaire en pratique.

d. Enfin, une précision a été apportée concernant le **motif justificatif en faveur des médias** (let. d), selon laquelle un intérêt privé prépondérant doit être présumé non seulement lorsque les données personnelles sont traitées exclusivement en vue de leur publication dans la partie rédactionnelle d'un média à caractère périodique, mais aussi lorsque les données ne sont pas publiées et servent uniquement d'instrument de travail personnel. Il est

44 Cf. les « Codes de conduite » de l'IG Wirtschaftsauskunfteien, état au 21 avril 2020 (https://bit.ly/3juFcyn (état au 9 mars 2021)).

ainsi précisé que les enquêtes ou les données non publiées (p. ex. celles d'autres personnes qui ne sont pas mentionnées dans un article) sont également couvertes – même si elles sont partagées au sein de la rédaction (et ne relèvent donc pas de l'exception de l'usage personnel au sens de l'art. 2 al. 2 let. a nLPD).

E. Mesures visant à garantir la protection des données

1. Privacy by Design

[43] L'art. 7 nLPD réglemente désormais les deux concepts clés de « Privacy by Design » et « Privacy by Default », le second étant inclus dans le premier. La théorie sous-jacente est la suivante : tous les problèmes de protection des données seraient résolus si les systèmes utilisés pour traiter les données personnelles étaient techniquement **conçus dès le départ de manière à respecter la protection des données**. La mise en œuvre de cette théorie est toutefois irréaliste, car les exigences sont beaucoup trop complexes et diverses. Si l'on ramène le concept de « Privacy by Design » à un degré réaliste, il s'agit en fin de compte de faire du neuf avec du vieux. Les responsables du traitement sont tenus de faire la même chose qu'auparavant, à savoir mettre en œuvre en temps utile les mesures techniques et organisationnelles appropriées afin que le traitement envisagé respecte les prescriptions en matière de protection des données. Hormis l'ajout du concept de « Privacy by Default » à l'al. 3 (cf. N 38 ss), l'art. 7 nLPD n'impose pas de nouvelles obligations aux responsables du traitement. Auparavant, l'obligation de protéger les données dès la conception figurait à l'art. 7 LPD. Cet article a été remplacé par l'art. 8 nLPD qui se limite désormais à la sécurité des données au sens strict. L'art. 7 nLPD n'est plus un principe de traitement (il n'est pas mentionné à l'art. 30 al. 2 let. a nLPD), c'est-à-dire que l'absence de mesures n'entraîne plus nécessairement – comme c'était le cas auparavant – une atteinte à la personnalité. Cela dit, la violation de l'art. 7 nLPD peut, en tant qu'obligation légale de diligence, avoir un effet au moins similaire à celui d'une responsabilité causale légère, si les mesures nécessaires pour éviter les atteintes à la personnalité n'ont pas été prises. Dans le cas contraire, la violation du concept de « Privacy by Design » ne peut être sanctionnée, sauf si le PFPDT prend des mesures à l'encontre d'un responsable du traitement dans un cas individuel et rend une décision en ce sens.

[44] Il appartient au responsable du traitement de décider des **mesures** qu'il souhaite mettre en place. A cet égard, il doit dans un *premier temps* définir tous les paramètres essentiels (du point de vue de la protection des données) du traitement en question. Dans un *deuxième temps*, il doit examiner de quelle manière il peut s'assurer que le traitement se déroule comme il l'a prévu et que toutes les prescriptions de protection des données seront respectées. Les moyens dont il dispose pour y parvenir sont, par exemple : les déclarations de protection des données, les directives internes, la mise en place de possibilités d'opposition, des offres « self-service » pour l'exercice des droits des personnes concernées, l'utilisation du chiffrement, les processus internes visant à limiter les finalités d'utilisation, la conception des applications de manière à éviter la collecte de données personnelles, l'automatisation de l'effacement des données, les mesures visant à interdire la ré-identification, les règles de responsabilité, la documentation des processus, l'évaluation des taux d'erreur à des fins d'assurance qualité, les mesures visant à empêcher les copies de données non synchronisées, et les règles sur la durée de conservation des données. L'accord entre les responsables conjoints du traitement, prévu par l'art. 26 RGPD, peut également être une mesure

au sens de l'art. 7 al. 1 et 2 nLPD. Dans un *troisième temps*, il conviendra pour le responsable du traitement de mettre en œuvre ces mesures.

[45] Contrairement au concept original de « Privacy by Design », il ne s'agit plus seulement de la conception des ordinateurs, **mais de tout ce qui est lié au traitement des données personnelles** (processus, responsabilités, ressources, etc.). Il suffit de prendre des mesures appropriées. Celle-ci doivent toutefois correspondre à l'« état de la technique », c'est-à-dire à ce qui s'est avéré efficace dans la pratique. La garantie de « conformité » doit (logiquement) être continue, depuis la phase de planification jusqu'à la fin du traitement des données. Contrairement à ce qui est prévu dans le RGPD, toutefois, le responsable du traitement n'est pas tenu de documenter ses activités selon l'art. 7 al. 1 et 2 nLPD. Un pendant au **principe de responsabilité** (« accountability ») de l'art. 5 al. 2 RGPD a été délibérément omis dans la nLPD, alors qu'il figurait encore dans l'avant-projet.

[46] Par « **prescriptions de protection des données** », il faut comprendre toutes les prescriptions qui garantissent la protection des données personnelles dans le cadre d'un traitement spécifique de données (p. ex. les principes de traitement, les conditions applicables à la sous-traitance, les règles relatives à la transmission de données personnelles à l'étranger, ainsi que le droit d'accès aux données, le droit de communiquer les données et le droit d'opposition). Cela ne comprend pas l'obligation de tenir un registre des activités de traitement, l'obligation de signaler les violations de la sécurité des données et l'obligation de réaliser une analyse d'impact relative à la protection des données.

2. Privacy by Default

[47] L'obligation de « Privacy by Default » est nouvelle dans la nLPD. Sa portée est toutefois limitée. Lorsqu'un responsable du traitement offre plusieurs options pour le traitement des données personnelles dans le cadre d'un service, d'un logiciel ou d'un appareil et que l'utilisateur a la possibilité de régler lui-même ces options *via* les paramètres de protection des données, **le paramètre par défaut doit être le moins étendu**. Lorsqu'un responsable du traitement n'offre aucune option (technique) à l'utilisateur pour contrôler lui-même le traitement de ses données, il ne peut logiquement effectuer de réglage *par défaut* et donc l'obligation ne s'applique pas.

[48] Un traitement de données effectué sur la base du consentement de la personne concernée ne donne pas lieu à un paramétrage par défaut. De même, il n'y a pas de paramétrage par défaut lorsqu'une personne concernée se voit accorder un droit d'opposition, même si ce droit peut être exercé dans le cadre d'un service en ligne au moyen d'une fonction technique (par ex. un bouton « opt-out »). L'obligation de « Privacy by Default » n'oblige pas non plus le responsable du traitement à offrir des **choix** aux utilisateurs (p. ex. son service en ligne ou son appareil). Toutefois, s'il le fait, tout paramètre par défaut doit être défini de manière à limiter le traitement au « minimum requis par la finalité poursuivie ».

[49] Le terme « **finalité poursuivie** » désigne l'*ensemble* des finalités de tous les traitements de données que le responsable du traitement entend effectuer ou proposer. Ce n'est que de cette manière que la norme a un sens. Le terme « minimum » fait référence à la moindre atteinte à la personnalité, et pas seulement au traitement dans le cadre duquel un minimum de données (en termes de volume) est traité, comme le préconise le message du Conseil fédéral[45]. Là encore, il

45 FF 2017 6649.

appartient au responsable du traitement de fixer les paramètres minimums du traitement qu'il est prêt à offrir. Le fait que l'interférence la moins intrusive avec la personnalité doive être prédéfinie ne concerne que la personnalité de la personne qui peut effectuer les réglages, à l'exclusion de celle des autres personnes concernées.

[50] L'obligation de « Privacy by Default » n'empêche pas non plus de pré-cocher la case d'une déclaration de consentement en ligne. En principe, cela reste autorisé par la nLPD, contrairement au RGPD. En outre, l'obligation de fournir un préréglage respectueux de la protection des données ne s'applique pas **si l'utilisateur en décide autrement** (art. 7 al. 3 *in fine* nLPD). Si, par exemple, lors de l'inscription à un service en ligne, l'utilisateur est invité à choisir le paramètre qu'il souhaite, il peut également se voir proposer des paramètres qui ne répondent pas aux exigences minimales, c'est-à-dire que les options correspondantes peuvent être sélectionnées par défaut. Si, en revanche, l'utilisateur peut passer les différents paramètres de réglages sans avoir fait de choix, le réglage par défaut doit correspondre à l'interférence la moins intrusive avec la personnalité.

[51] Par ailleurs, l'art. 7 al. 3 nLPD ne contient **aucune interdiction de couplage** (cf. aussi N 30) : le responsable du traitement peut donc décider qu'un traitement de données particulier ne peut être choisi que si d'autres traitements de données sont également autorisés en même temps. Cette possibilité sera au plus limitée par les principes de proportionnalité ou par les exigences en matière de consentement volontaire. L'exemple de la boutique en ligne, cité dans le message du Conseil fédéral[46], qui autorise les clients à faire des achats même sans créer un profil d'utilisateur, est en ce sens erroné, car il n'y a tout simplement pas de réglage par défaut.

[52] Au demeurant, la violation de l'art. 7 al. 3 nLPD n'entraîne pas de conséquences juridiques directes. L'application de la loi sera donc principalement entre les mains du PFPDT.

3. Sécurité des données

[53] En tant que principe de traitement, l'art. 8 nLPD prévoit que le responsable du traitement et – contrairement à l'art. 7 nLPD – le sous-traitant doivent garantir une sécurité adéquate des données par des **mesures techniques et organisationnelles**. Contrairement à la LPD actuelle, cette disposition ne couvre que la sécurité des données, c'est-à-dire la protection des données personnelles au regard de leur confidentialité, leur intégrité et leur disponibilité. Les mesures visant à prévenir d'autres violations de la protection des données sont prévues à l'art. 7 al. 1 et 2 nLPD. Quant aux exigences en matière de sécurité des données, elles ne changent pas par rapport à la LPD actuelle (et aussi par rapport au RGPD).

[54] Les mesures typiques pour assurer une sécurité adéquate des données comprennent, entre autres, les restrictions d'accès, les filtres (p. ex. les pare-feu), la pseudonymisation, y compris le chiffrement des données, l'enregistrement, les sauvegardes, les techniques d'élimination sécurisée, la surveillance, les systèmes d'alarme, ainsi que les règlements et directives, la formation, la sélection et la désignation de sous-traitants, les contrats régissant le traitement ou la confidentialité des données, la documentation, les contrôles, les tests d'intrusion et les règles de responsabilité.

46 FF 2017 6649.

[55] La loi ne prescrit aucune mesure spécifique. Les mesures ne doivent pas non plus offrir une **protection absolue** ; elles doivent plutôt, d'un point de vue objectif, être raisonnablement proportionnées au risque de violation de la sécurité des données (sur ce terme, cf. N 160). En cas de violation, la nLPD prévoit une obligation de notification (N 160 ss). L'art. 8 nLPD ne prévoit pas d'obligation de documentation spécifique, mais une telle obligation peut en découler de manière indirecte au sein des grandes entreprises, car la sécurité des données ne peut être raisonnablement garantie sans documentation des mesures de protection.

[56] Contrairement à la LPD actuelle, la violation intentionnelle de l'art. 8 nLPD peut également être sanctionnée pénalement par une **amende** pouvant aller jusqu'à CHF 250'000. Une telle amende ne pourra toutefois être infligée que si les « exigences minimales », telles qu'elles seront définies par le Conseil fédéral dans l'ordonnance, auront été intentionnellement ignorées (art. 61 let. c nLPD). Il faut s'attendre à ce que de telles amendes ne soient infligées que lorsqu'un responsable du traitement ou un sous-traitant ne garantit pas le niveau minimum de sécurité des données nécessaire. Si, malgré les mesures prises, une violation de la sécurité des données survient, cela ne justifie pas une sanction et ne constitue pas nécessairement une violation de l'art. 8 nLPD. Il existera toujours un risque résiduel.

F. Sous-traitance

[57] La « sous-traitance » est courante dans l'économie actuelle basée sur la division du travail. En substance, il s'agit d'un responsable du traitement qui fait effectuer son *propre* traitement de données par un tiers *pour son compte.* Comme nous l'avons déjà expliqué ci-dessus dans le cadre des notions de « responsable du traitement » et de « sous-traitant » (N 13 ss), tout traitement de données (y compris de données personnelles) confié à un tiers ne constitue pas nécessairement un cas de sous-traitance. La sous-traitance (p. ex. l'externalisation des fonctions informatiques à un fournisseur de services en nuage ou l'exécution d'un mailing publicitaire) **est en principe toujours autorisé en vertu de la nLPD sans qu'il soit nécessaire d'obtenir le consentement des personnes concernées**. Les conditions de la sous-traitance ont toutefois été légèrement renforcées.

[58] L'externalisation doit, bien entendu, respecter les principes de traitement et en particulier être proportionnée[47]. Les dispositions relatives à l'exportation de données (N 64 ss) doivent également être respectées. En revanche, il n'est **pas nécessaire d'informer** de la sous-traitance dans le cadre de la marche normale des affaires. Une exception à cette règle a été introduite avec la révision de l'art. 19 al. 2 nLPD, lequel dispose désormais que le responsable du traitement doit informer la personne concernée des éventuels destinataires des données. Les sous-traitants font partie des destinataires au sens de cette disposition[48]. Il en va de même pour le droit d'accès. En principe, il n'est pas nécessaire de mentionner les sous-traitants nommément. Si les conditions de la sous-traitance sont remplies, le sous-traitant est assigné au responsable du traitement aux fins de la protection des données – il n'y a pas de communication à un « tiers », ni de changement de finalité. Le sous-traitant peut invoquer les mêmes motifs justificatifs que le responsable du

47 Dans certains cas, l'externalisation peut même être conseillée, par exemple, si elle permet d'assurer le niveau de sécurité informatique nécessaire et que le responsable du traitement ne dispose pas des compétences techniques nécessaires en la matière.

48 FF 2017 6669.

traitement. Les employés du responsable du traitement (y compris les tiers intégrés dans l'entreprise et agissant sur instruction et sous la supervision du responsable du traitement, tels que les consultants) ne sont techniquement pas des sous-traitants, mais les règles relatives aux sous-traitants leur sont applicables par analogie ; dans le RGPD, ils sont régis séparément à l'art. 29 RGPD. Si un sous-traitant traite les données de clients (également) **à ses propres fins**, il devient le responsable du traitement ; cela est admissible du point de vue de la protection des données, à condition qu'il soit correctement réglementé.

[59] Les **conditions** de la sous-traitance n'ont en principe pas changé, mais une exigence a été ajoutée (N 60). Ces conditions sont énoncées à l'art. 9 nLPD. En substance, le responsable du traitement doit s'assurer – généralement par le biais d'un contrat et par une sélection, des instructions et un contrôle minutieux – que le sous-traitant n'effectue que le traitement (conforme à la protection des données) qu'il a défini et qu'il peut remplir ses obligations en vertu de la LPD. Ces exigences sont mises en œuvre au moyen d'un droit d'instruction et de contrôle, ce dernier étant également assorti d'une obligation contractuelle d'assistance. Contrairement à l'art. 28 al. 3 RGPD, l'art. 9 nLPD ne définit pas les éléments contractuels qui doivent être régis par le contrat entre le responsable du traitement et le sous-traitant. En droit suisse, le responsable du traitement s'oriente généralement par rapport aux exigences du RGPD afin de respecter ses obligations. L'art. 9 nLPD lui donne toutefois plus de liberté quant à la *manière* dont il s'en assure (p. ex. le respect des droits de la personne concernée ou la restitution des données à la fin du contrat). Le sous-traitant est directement soumis à certaines obligations, telles que l'obligation d'assurer la sécurité des données conformément à l'art. 8 nLPD (et donc aussi la confidentialité) et l'obligation d'annoncer les violations de la sécurité des données (art. 24 nLPD). Si le sous-traitant est situé à l'étranger, un contrat sera souvent nécessaire pour des raisons de force exécutoire. La conclusion de tels « contrats de sous-traitance » avec les éléments requis par l'art. 28 al. 3 RGPD, est désormais pratique courante ; les principaux points de discussion sont de savoir qui doit supporter les coûts, jusqu'où l'intervention est possible et jusqu'où les instructions peuvent aller. Les fournisseurs de services dans les nuages standardisés ne permettent souvent pas à leurs clients de réaliser des audits sur place, préférant s'en remettre à des audits collectifs réalisés par des sociétés d'audits indépendantes pour leur compte et qui sont accompagnés de certificats, d'attestations ou de rapports d'essai correspondants. Le droit de donner des instructions est également « unifié » dans la mesure où les instructions contenues dans le contrat et les paramètres et les utilisations définis par le client pour le service en ligne en question sont considérés comme les « seules et ultimes » instructions données par le client, c'est-à-dire qu'aucune autre instruction ne pourra être donnée. Si cela n'est pas suffisant pour le client, il doit résilier le contrat. Jusqu'à présent, de tels accords étaient autorisés selon les circonstances et ils continueront à l'être sous la nLPD. Comme dans le cadre du RGPD, il est toujours permis – et également assez courant – de limiter la responsabilité du sous-traitant. En revanche, il n'est pas permis d'exiger du sous-traitant qu'il paie les amendes prévues par la nLPD, car elles sont de nature personnelle et que, partant, cela irait à l'encontre de leur objectif (N 191).

[60] L'art. 9 al. 3 nLPD est nouveau. Il prévoit que le sous-traitant ne peut sous-traiter un traitement à un tiers (« **sous-traitant ultérieur** », en anglais « sub-processor ») qu'avec l'autorisation préalable du responsable du traitement. Cette disposition correspond en substance à l'art. 28 al. 2 RGPD ; la FINMA prévoit une réglementation similaire, quoique légèrement allégée, dans

sa circulaire sur l'externalisation dans le secteur des banques et des entreprises d'assurances[49]. Il n'y a pas de sous-traitance lorsqu'un sous-traitant fait appel à des tiers qui ne sont eux-mêmes pas considérés comme des sous-traitants (p. ex. son propre personnel ou des consultants)[50]. Par « autorisation », on entend l'autorisation du responsable du traitement dans un cas individuel (lorsqu'il connaît le tiers nommément) ou en général (lorsqu'il ne connaît pas le tiers). Dans le secteur privé, l'autorisation n'est soumise à aucune exigence de forme. Dans le cas d'une autorisation générale, le sous-traitant est tenu d'informer le responsable du traitement de l'identité du tiers (et, en règle générale, aussi du pays dans lequel il se trouve et de l'activité de sous-traitance) avant la sous-traitance en question, afin que le responsable du traitement puisse s'y opposer le cas échéant[51]. Une telle « autorisation avec réserve d'objection » est principalement revendiquée par les fournisseurs de services standardisés (p. ex. les services en nuage), car une autorisation individuelle ne serait pas praticable pour eux sur le plan logistique. Le délai de préavis n'est pas défini dans la loi ; en pratique, il va de sept jours à six mois. Même s'il n'y a généralement pas d'objection, le délai de préavis doit laisser suffisamment de temps pour évaluer la sous-traitance ultérieure et il doit pouvoir être exercé de manière réaliste par le responsable du traitement. Dans le cas des services standardisés, le droit d'opposition prend généralement la forme d'un droit de résiliation extraordinaire. Les informations peuvent être fournies par le biais d'une liste de sous-traitants ultérieurs, publiée sur le site Internet, avec notification automatique en cas de changement. Il convient également de fournir des informations sur les autres sous-traitances ultérieures (c'est-à-dire si le sous-traitant ultérieur implique à son tour d'autres sous-traitants), ce qui est souvent négligé dans la pratique. La disposition de l'art. 9 al. 3 nLPD s'applique également à la sous-traitance au sein d'un même groupe de sociétés. Toutefois, l'art. 9 al. 3 nLPD ne prévoit pas un droit de révoquer ultérieurement un sous-traitant. De par sa nature juridique, la disposition est une interdiction de droit public ; sa violation ne conduit pas directement à une atteinte à la personnalité, mais indirectement par le biais de l'art. 6 al. 1 nLPD. Il découle de l'art. 9 al. 1 et 2 (et non de l'al. 3) nLPD que le responsable du traitement doit veiller à ce que les exigences des al. 1 et 2 soient respectées tout au long de la chaîne de sous-traitance. Cela était déjà le cas auparavant et ne change donc pas. Cependant, la nLPD n'exige pas que le responsable du traitement ait des droits d'instruction et de contrôle directs vis-à-vis du sous-traitant ultérieur (le RGPD d'ailleurs non plus).

[61] Désormais, la violation intentionnelle de l'art. 9 al. 1 et 2 (mais non de l'al. 3) nLPD par le responsable du traitement est punie d'une **amende** pouvant aller jusqu'à CHF 250'000 (art. 61 let. b nLPD). Il est donc dans l'intérêt des responsables du traitement d'obliger les sous-traitants à se conformer à leurs exigences. Les sous-traitants n'encourent toutefois aucun risque de responsabilité pénale au titre de cette disposition, même en cas de sous-traitance ultérieure. Il n'y a pas non plus de risque de responsabilité pénale dans les cas où l'art. 9 nLPD s'applique par analogie. En cas d'atteinte à la personnalité, la personne concernée peut déposer plainte contre toute personne qui a participé à l'atteinte, y compris les sous-traitants. En ce qui concerne le responsable du traitement, la responsabilité civile de l'employeur[52] s'ajoute à la responsabilité pénale prévue à l'art. 61 let. b nLPD. Le responsable du traitement à la possibilité de s'exonérer de sa respon-

49 Circulaire 2018/3 de la FINMA sur l'externalisations dans le secteur des banques et des entreprises, ch. 33.

50 FF 2017 6652.

51 FF 2017 6651.

52 Art. 55 CO.

sabilité en apportant la preuve libératoire ; des règles similaires s'appliquent dans le cadre du RGPD[53]. S'il existe une relation contractuelle entre le responsable du traitement et la personne concernée, la responsabilité des auxiliaires peut également entrer en ligne de compte[54].

[62] En pratique, les sous-traitants en Suisse sont souvent confrontés à des **contrats de sous-traitance au sens de l'art. 28 RGPD**. L'adoption de ces contrats est toujours possible dans le cadre de la nLPD, mais ils doivent – comme c'est le cas aujourd'hui – être adaptés à la législation suisse. *Premièrement*, les références au RGPD doivent être complétées par des références correspondantes à la LPD (ou par l'indication « droit applicable à la protection des données »). *Deuxièmement*, la communication des données à l'étranger doit être adaptée de manière à ce que les exportations de données de la Suisse soient également couvertes conformément à la LPD. Et, *troisièmement*, dans les relations internationales, le champ d'application doit être formulé de manière à ce que tous les cas de sous-traitance relevant de la LPD soient couverts, et pas seulement ceux qui sont soumis au RGPD.

[63] Au demeurant, la nLPD ne modifie pas l'**obligation de garder le secret** prévue à l'art. 9 al. 1 let. b nLPD. Pour de plus amples informations à ce sujet, le lecteur est renvoyé à une autre contribution de l'auteur de cet article[55].

G. Exportation des données

1. Approche réglementaire générale

[64] Les dispositions relatives à la **communication de données personnelles à l'étranger** au sens des art. 16 ss nLPD ont été adoptées sans difficulté par le Parlement. Une suppression dans le domaine des obligations de notification a été ajoutée et, de manière générale, la nouvelle réglementation sur les exportations est un peu plus libérale que les dispositions actuelles. Alors que, par le passé, les contrats relatifs à la communication transfrontière de données à des pays tiers peu sûrs (du point de vue de la protection des données) devait être déclarés *pro forma* au PFPDT, cela ne sera plus nécessaire dans le cadre de la nLPD.

[65] Sur le principe, la règlementation ne change pas beaucoup. Il ne reviendra plus à l'exportateur de données d'évaluer si un pays tiers offre un niveau de protection des données adéquat, mais au **Conseil fédéral, qui décidera de manière contraignante**, comme le fait la Commission européenne dans l'EEE[56]. La Suisse elle-même attend actuellement que la Commission européenne se prononce sur sa propre adéquation. Dans l'esprit d'une application autonome du droit européen et afin de ne pas créer une porte dérobée pour l'exportation de données depuis l'EEE, on peut supposer que le Conseil fédéral ne reconnaîtra comme adéquats que les États qui le sont également selon l'avis de la Commission européenne. C'est précisément pour cette raison que le

53 Art. 82 al. 2 et 3 RGPD.

54 Art. 101 CO.

55 David Rosenthal, Mit Berufsgeheimnissen in die Cloud : So geht es trotz US CLOUD Act, in : Jusletter du 10 août 2020.

56 Le Conseil fédéral adoptera vraisemblablement la liste des pays du PFPDT : https://www.edoeb.admin.ch/edoeb/fr/home/protection-des-donnees/handel-und-wirtschaft/uebermittlung-ins-ausland.html (état au 9 mars 2021).

PFPDT a récemment supprimé le *Privacy Shield* pour les États-Unis (N 74) de sa liste des États. Auparavant, le *Privacy Shield* servait de base pour accepter l'adéquation des États-Unis[57].

[66] Les dispositions des art. 16 ss nLPD n'entrent en ligne de compte que si des données personnelles sont communiquées depuis la Suisse à un destinataire à l'étranger. Par définition, la « communication » suppose que le cercle des personnes détenant les informations en question soit élargi. Ainsi, la personne qui accède à sa propre boîte email depuis l'étranger ou emporte avec elle des données sur son ordinateur portable lors d'un voyage à l'étranger ne communique pas encore des données personnelles au sens des art. 16 ss nLPD. Elle ne le fait que si elle montre les données personnelles à une personne à l'étranger. L'**accès à distance** est également considéré comme une communication à l'étranger : la personne qui met à la disposition d'une autre personne des données personnelles stockées sur un serveur en Suisse, mais accessible à distance (*remote access*), communique à cette dernière des données personnelles. Comme auparavant, en vertu d'une règle spéciale, la publication de données personnelles sous forme électronique n'est pas assimilée à une communication à l'étranger, même si ces données peuvent être consultées depuis l'étranger (art. 18 nLPD). En revanche, la communication de données personnelles au sein d'une même entreprise n'exclut pas l'application des art. 16 ss nLPD. Ainsi, la personne qui met des données personnelles de Suisse à la disposition de sa propre succursale à l'étranger doit se conformer aux art. 16 ss nLPD.

[67] Le concept de la LPD diffère (encore) quelque peu de celui du RGPD. Selon l'opinion dominante, dans le cadre du RGPD, les données personnelles sont transférées en vue de leur traitement ultérieur dans le pays tiers (de destination) ; il ne s'agit donc pas seulement d'une communication transfrontalière depuis le territoire national. Si, dans la plupart des cas, cette distinction n'a pas d'importance, elle devient pertinente lorsque les données personnelles sont **transférées ultérieurement d'un pays tiers à un autre pays tiers** : dans ces cas, les art. 44 ss RGPD trouvent application, mais pas l'art. 16 nLPD, car cette disposition ne s'applique qu'à la communication de données *depuis la Suisse.* Ainsi, si une entreprise suisse collecte des données personnelles en Allemagne et les exporte en Inde sans passer par la Suisse, l'art. 16 nLPD ne s'applique pas, du moins selon l'interprétation actuelle[58]. En revanche, si une entreprise suisse traite des données personnelles en Suisse et les exporte en Inde, la norme parallèle de l'art. 44 RGPD s'applique, même si les données n'auront jamais été transmises depuis le territoire de l'EEE – à condition toutefois que le traitement des données soit soumis au RGPD.

[68] En principe, les données personnelles peuvent donc toujours être communiquées, sans autre formalité, à tous les États qui disposent d'une **législation assurant un niveau de protection des données adéquat**, selon (désormais) la liste du Conseil fédéral. Des divergences par rapport aux décisions d'adéquation de la Commission européenne sont à prévoir dans les cas où la loi sur la protection des données d'un État tiers accorderait un traitement préférentiel aux données de personnes ressortissantes de l'EEE, mais pas de la Suisse[59]. Quoi qu'il en soit, tous les pays de l'EEE offrent un niveau de protection adéquat, tout comme le Royaume-Uni [*depuis le Brexit*], qui a

57 PFPDT : Prise de position sur la transmission de données personnelles vers les États-Unis et d'autres États n'offrant pas un niveau adéquat de protection des données au sens de l'art. 6 al.1 LPD, 8 septembre 2020.

58 Toutefois, un tel transfert ultérieur (*onward transfer*) peut être prohibé par l'accord de protection des données requis ou par la législation locale en matière de protection des données (p. ex. RGPD), car il doit également être respecté par les sous-traitants.

59 Par exemple, jusqu'à présent dans le cas du Japon.

adopté la législation européenne sur la protection des données[60]. Les dispositions de la Convention 108 révisée sur la protection des données du Conseil de l'Europe constituent – officieusement – le standard minimum à respecter pour qu'un État soit considéré comme offrant un niveau de protection adéquat.

[69] Jusqu'à récemment, les États-Unis constituaient un cas particulier : ils étaient aussi considérés comme un État offrant un niveau de protection adéquat, mais uniquement en ce qui concerne les entreprises qui s'étaient auto-certifiées dans le cadre du « *Privacy Shield Framework* »[61]. Les principaux fournisseurs américains de services en ligne, tels que Google, Amazon, Facebook et Microsoft, en sont des exemples. L'auto-certification équivalait à une protection légale des données dans la mesure où ces entreprises avaient fait la promesse quasi-publique de respecter les principes de la protection des données européenne et pouvaient donc être poursuivies en vertu du droit de la concurrence déloyale en cas de violation de leur promesse. Le Conseil fédéral devra décider si les communications de données dans des cas analogues au *Privacy Shield* (si tant est qu'il existe encore, N 74) seront à l'avenir considérées comme relevant de l'art. 16 al. 1 nLPD, comme auparavant, ou si elles seront systématiquement couvertes par l'exception prévue à l'art. 16 al. 3 nLPD (N 67).

[70] Dans la pratique, lors de l'adoption d'accords et de déclarations de protection des données formulés spécifiquement pour le RGPD, il faut veiller à ce que les formulations soient étendues de manière à ce que, d'une part, les exportations de Suisse soient également couvertes et, d'autre part, que les règlementations s'appliquent également aux données provenant de Suisse. Le RGPD utilise le terme « pays tiers » pour désigner tous les pays en dehors de l'EEE. Du point de vue de l'EEE, la Suisse est un pays tiers. Du point de vue de la Suisse, en revanche, tous les pays autres que la Suisse sont des pays tiers. Cet aspect doit aussi être pris en compte dans le cadre des déclarations de protection des données car, selon l'art. 19 al. 4 nLPD, tous les pays (ou régions) vers lesquels des données personnelles sont exportées de Suisse doivent désormais être communiqués aux personnes concernées.

2. Dérogations

[71] Si un État ne dispose pas d'une législation assurant un niveau de protection adéquat, le transfert de données vers cet État peut quand même avoir lieu à condition qu'un contrat approprié puisse être conclu avec les destinataires des données, en vertu duquel la protection des données est assurée contractuellement dans la mesure nécessaire. Dans la pratique, les contrats les plus fréquemment utilisés sont les **clauses contractuelles types de la Commission européenne**, lesquelles sont *[dans leur version actuelle]* à la disposition des sous-traitants et des responsables du traitement en tant que destinataires[62]. Elles peuvent également être utilisées pour les relations contractuelles suisses. Une adaptation des références à la nLPD et à ses définitions peut s'avérer utile, mais n'est pas obligatoire, pour autant qu'il ressorte de manière suffisamment claire que

60 Du point de vue de l'EEE, cependant, les exportations de données vers le Royaume-Uni nécessiteront une décision d'adéquation officielle de la Commission européenne. *[La Commission européenne a récemment publié un projet de décision d'adéquation concernant le Royaume-Uni.]*

61 Privacy Shield List, https://www.privacyshield.gov/list (état au 9 mars 2021).

62 Les clauses contractuelles types de la Commission européenne sont disponibles sur le site suivant : https://bit.ly/3lt6Yvq (état au 9 mars 2021) ; toutefois, de nouvelles clauses contractuelles types devraient être publiées par la Commission européenne prochainement.

les transferts de données depuis la Suisse sont également couverts. Tant que les clauses types de protection des données sont préalablement reconnues, établies ou approuvées par le PFPDT – ce qui était le cas jusqu'à présent des clauses contractuelles types de la Commission européenne –, aucune autre mesure n'est requise. L'obligation de déclarer ces garanties contractuelles au PFPDT a été abandonnée dans le cadre de la nLPD (art. 16 al. 2 let. d nLPD). Cela correspond aux dispositions du RGPD.

[72] Les clauses types sont suffisantes dans la plupart des cas pour autant qu'elles ne soient pas modifiées dans leurs aspects relatifs à la protection des données. Si elles ne conviennent pas, il existe deux alternatives, à savoir établir un contrat individuel garantissant contractuellement une protection adéquate des données ou utiliser des ***Binding Corporate Rules*** (BCR) :

a. La première alternative est une liberté suisse que le RGPD ne connaît pas sous cette forme. Elle nécessite que le contrat soit communiqué au préalable au PFPDT afin qu'il puisse l'examiner et le commenter. Toutefois, l'approbation formelle du PFPDT n'est pas nécessaire.
b. Les BCR, quant à elles, sont connues du RGPD. Il s'agit de règles internes à un groupe d'entreprises en matière de protection des données qui permettent aux entités du groupe situées dans des pays tiers peu sûrs (du point de vue de la protection des données) de garantir un niveau de protection adéquat aux données transférées. Ces règles peuvent être étendues ou limitées à certains domaines. En général, toutes les entités du groupe concluent un contrat régissant la protection des données, similaire aux clauses contractuelles types. L'avantage des BCR est que, d'une part, elles permettent de s'écarter des clauses types reconnues par le PFPDT et, d'autre part, elles peuvent être rédigées de manière plus générique pour un grand nombre de traitements de données au sein du groupe (elles ne sont pas limitées à des traitements spécifiques, comme c'est généralement le cas des clauses types). Il existe des BCR tant pour les transferts de données entre responsables du traitement que pour les transferts de données entre sous-traitants et sous-traitants ultérieurs (appelés *Processor BCR*)[63]. Auparavant, en Suisse, les BCR devaient uniquement être communiquées au PFPDT. Désormais – par analogie avec l'art. 47 RGPD – elles sont soumises à l'approbation du PFPDT (art. 16 al. 2 let. e nLPD), étant entendu que les approbations délivrées en vertu du RGPD peuvent également être reconnues. Cela dit, les BCR ont jusqu'à présent joué un rôle secondaire en Suisse, car elles sont relativement complexes et n'apportent souvent aucun avantage réel. Les accords de transfert de données à l'échelle du groupe, basés sur les clauses contractuelles types de l'UE, sont souvent beaucoup plus simples en pratique. Ils couvrent aussi souvent d'autres exigences en matière de protection des données, comme par exemple la réglementation de la sous-traitance et les responsabilités conjointes au sein du groupe.

[73] En théorie, la protection des données dans les pays tiers qui ne garantissent pas un niveau de protection adéquat pourrait également être assurée par d'autres mécanismes que des garanties contractuelles, par exemple par des restrictions techniques ou par des **systèmes d'autocertifica-**

63 Ce système est souvent utilisé par des prestataires de services actifs au niveau international qui concluent des contrats avec des clients par l'intermédiaire de leurs entreprises locales en Europe. Les entreprises européennes transfèrent ensuite, dans le cadre du traitement des données personnelles, les données des clients vers les États-Unis ou d'autres pays tiers n'offrant pas un niveau de protection adéquat.

tion, comme dans le cas du *Privacy Shield* mentionné ci-dessus[64]. Si, auparavant, il n'y avait pas de conditions formelles à cet égard, désormais l'admission de ces autres « garanties » nécessite une décision du Conseil fédéral (art. 16 al. 3 nLPD). Le RGPD prévoit des exigences similaires pour les certifications, mais offre beaucoup moins de flexibilité (art. 46 al. 2 let. f RGPD).

[74] Alors qu'il était auparavant considéré comme acquis que les exportations de données vers des pays tiers peu sûrs (du point de vue de la protection des données) pouvaient être garanties de manière adéquate par le biais d'un contrat, cela n'est plus aussi clair pour certains experts et représentants d'autorités depuis la décision « **Schrems II** » de la CJUE du 16 juillet 2020[65]. Dans cette décision, la CJUE a rappelé que les contrats à eux seuls n'offrent pas nécessairement une protection suffisante parce que les autorités étrangères ne sont pas tenues de les respecter. Cette décision a été motivée par une disposition du droit américain qui permet aux services de renseignement américains d'accéder à des données personnelles provenant de l'étranger, même en l'absence d'un jugement dans ce sens, ce qui est contraire aux garanties constitutionnelles de l'UE. A la lumière de ces faits, la CJUE a révoqué la reconnaissance du *Privacy Shield* par la Commission européenne. Quant aux clauses contractuelles types de la Commission européenne (et des BCR), elles font l'objet de discussions au sein de l'EEE, notamment sur la question de savoir dans quels cas les mesures supplémentaires seront nécessaires pour continuer à pouvoir transmettre légalement des données personnelles aux États-Unis. Dans certains cas, il sera nécessaire de procéder à une analyse du risque réel d'accès par les autorités à l'étranger, d'utiliser de manière plus intensive le cryptage et d'adapter les contrats ou de relocaliser le traitement des données des États-Unis vers l'Europe. La discussion est actuellement toujours en cours, car les autorités de protection des données ne savent pas non plus ce qu'il faut faire. La Commission européenne devrait publier prochainement de **nouveaux contrats types**. Le nouvel art. 16 al. 2 nLPD laisse toutes les options ouvertes : si le législateur reconnaît le recours à des contrats pour sécuriser l'exportation de données vers des Etats tiers qui ne garantissent pas un niveau de protection adéquat, l'exportation ne sera autorisée que si elle permet effectivement de garantir « un niveau de protection approprié ». Dans la pratique, le PFPDT pourra donc facilement faire valoir que, dans certains cas, un contrat ou les BCR ne seront pas suffisants.

[75] Si ni un contrat ni les BCR n'entrent en considération, l'exportateur de données doit se contenter d'une des **autres dérogations** de l'art. 17 nLPD. Ces dérogations existaient aussi pour la plupart auparavant, mais le catalogue de cette disposition a été quelque peu élargi pour s'aligner sur le RGPD. L'exception du consentement est toujours prévue, mais celui-ci doit désormais être donné expressément – et non plus dans un cas individuel comme c'était le cas jusqu'à présent (let. a). En pratique, le consentement est rarement invoqué, car il signifie généralement que les données personnelles ne sont plus protégées à l'étranger, ce qui doit être porté à la connaisssance de la personne concernée. Toutefois, des gradations sont envisageables, comme l'utilisation de clauses contractuelles qui, bien qu'elles ne répondent pas aux exigences de l'art. 16 nLPD notamment à la lumière de « Schrems II », sont acceptées par les personnes concernées comme suffisantes. En pratique, le consentement n'est généralement pas pertinent, car il n'est souvent pas possible d'obtenir le consentement de toutes les personnes concernées. Au demeurant, si **une personne communique elle-même ses données personnelles à l'étranger** (p. ex. en les saisissant

64 FF 2017 6660.

65 Arrêt de la CJUE du 16 juillet 2020, C-3111/18 (« Schrems II »), para. 126 ss.

sur un site Internet étranger), cela ne constitue pas une communication au sens de l'art. 16 nLPD et le consentement n'est pas nécessaire pour l'exportation des données.

[76] Dans la pratique, les deux dérogations les plus importantes de l'art. 17 nLPD sont les suivantes :

a. Les données personnelles peuvent être transférées vers un pays tiers sans protection juridique adéquate des données, si la communication est en **relation directe avec la conclusion ou l'exécution d'un contrat** avec la personne concernée ou – ce qui est une nouveauté – avec une personne dans l'intérêt de laquelle le contrat doit être conclu ou exécuté (let. b). Cette dernière peut, par exemple, être un ayant droit économique ou un bénéficiaire dont les données personnelles doivent être communiquées à l'étranger par une banque dans le cadre de l'exécution d'une transaction. Auparavant, la communication de données de tiers était incluse dans l'exception. La formulation de la disposition correspondante de l'art. 31 al. 2 let. b nLPD ne va pas aussi loin, mais doit être comprise de la même manière ; la formulation plus large de l'art. 17 let. b nLPD est probablement due à un alignement sur l'art. 49 al. 1 let. b et c RGPD (qui prévoit les mêmes exceptions). Selon l'opinion dominante, l'expression « en relation directe » doit être comprise comme « nécessaire », soit, en définitive, exactement de la même manière que l'art. 31 al. 2 let. b nLPD. Le RGPD exige également que le transfert de données soit *nécessaire* à la conclusion ou à l'exécution du contrat, et pas seulement qu'il soit effectué *dans le cadre* de celui-ci. Il convient de noter que l'art. 17 al. 1 let. b nLPD admet dans ces cas une exportation des données sans le consentement de la personne concernée et sans contrat avec le destinataire. Cette disposition ne libère toutefois pas le responsable du traitement qui transfère les données à l'étranger de son obligation de transparence, ni – selon l'opinion dominante – de son obligation de veiller à ce que les données ne soient pas utilisées à d'autres fins.

b. Les données personnelles peuvent être transférées vers un pays tiers qui ne dispose pas de protection juridique adéquate des données si la communication est nécessaire à la constatation, à l'exercice ou à la défense d'un droit **devant un tribunal ou une autre autorité étrangère compétente** (art. 17 al. 1 let. c ch. 2 nLPD). La révision a ajouté un élargissement du champ d'application de cette exception à d'autres autorités compétentes, en plus des tribunaux. Cette modification revêt une importance pratique considérable, car le régime d'exportation antérieur de la LPD trouvait ses limites lorsque des entreprises suisses voulaient coopérer avec des autorités étrangères, par exemple dans le cadre d'une enquête administrative ou pénale. Dans ces cas, seule la communication de données personnelles dans le cadre de *procédures judiciaires* à l'étranger était possible (p. ex. dans le cadre des soumissions de preuves ou d'un *pre-trial discovery*). La plupart des interdictions judiciaires relatives à la divulgation de données d'employés ou de conseillers tiers par les banques suisse, dans le cadre du litige fiscal américain en Suisse étaient fondées sur cette lacune règlementaire (conditionnée par l'histoire) de l'ancienne LPD.
   Toutefois, l'exception étendue de la let. c ch. 2 ne signifie pas pour autant que les données personnelles peuvent être librement communiquées à des autorités étrangères. D'une part, les principes de traitement et les autres principes de la LPD (y compris le principe de transparence et le droit d'opposition) continuent de s'appliquer et, d'autre part, même en cas de communication, il faut veiller à ce qu'aucune utilisation abusive des données personnelles ne soit faite par la suite. Dans les procédures judiciaires, cela est garanti par le tribunal, par

les règles de procédure et les ordonnances de clôture et – lorsque la loi ne prévoit pas déjà elle-même la confidentialité – par les parties adverses, par des accords de confidentialité correspondants ou des ordonnances du tribunal. Aux États-Unis, par exemple, les *protective orders* étendus aux données personnelles pour les *enquêtes préalables au procès*, c'est-à-dire des accords de confidentialité approuvés par les tribunaux et assortis de restrictions d'utilisation, ont été introduits précisément à ces fins.

[77] L'art. 17 nLPD prévoit d'autres exceptions, notamment concernant la sauvegarde d'**intérêts publics prépondérants** (les exigences sont ici très élevées selon la pratique des tribunaux), la protection de l'**intégrité corporelle**, les données personnelles **rendues accessibles à tout un chacun** par la personne concernée elle-même et les données figurant dans un **registre** prévu par la loi. L'art. 17 nLPD ne prévoit pas la communication de données à l'étranger fondée sur une obligation légale. Toutefois, si une disposition du droit suisse permet ou exige la communication de données personnelles à un pays tiers qui ne dispose pas d'un niveau de protection adéquat, elle devrait en principe prévaloir sur les art. 16 ss nLPD en tant que *lex specialis.*

[78] L'exigence selon laquelle le responsable du traitement ou le sous-traitant doit avoir informé le PFPDT de l'application de certaines exceptions a été supprimée à juste titre lors des débats parlementaires. Aujourd'hui déjà, l'obligation prévue à l'art. 19 nLPD d'informer la personne concernée (également) des exceptions prévues à l'art. 17 nLPD va plus loin que le RGPD.

3. Sanctions

[79] Alors que, par le passé, la violation des dispositions de la LPD relatives à la communication de données personnelles à l'étranger n'avait généralement pas de conséquences, elle peut désormais être sanctionnée pénalement. Une personne privée qui communique intentionnellement des données personnelles à l'étranger en violation des art. 16 et 17 nLPD est punissable d'une **amende** pouvant aller jusqu'à CHF 250 000. Cela comprend également la violation de l'obligation de notification et d'autorisation. Toutefois, une plainte pénale est nécessaire, c'est-à-dire que la personne concernée doit agir. Le PFPDT lui-même ne peut pas déposer plainte pénale.

[80] La disposition pénale et les art. 16 et 17 nLPD s'appliquent non seulement aux responsables du traitement, mais **aussi aux sous-traitants**. Cela signifie qu'un sous-traitant en Suisse qui offre ses services à un responsable de traitement à l'étranger et qui, dans ce cadre, retransmet à ce dernier les données personnelles qui lui ont été préalablement communiquées, doit également respecter les dispositions des art. 16 et 17 nLPD. Jusqu'à présent, ce scénario avait été largement ignoré. Généralement, les contrats d'exportation de données sont conclus avec les sous-traitants en tant que destinataires des données personnelles, et non en tant qu'exportateur de celles-ci. En pratique, le problème est généralement résolu en droit suisse par le fait que, d'une part, la retransmission de données personnelles au responsable du traitement n'est pas considérée comme une communication au sens des art. 16 et 17 nLPD puisque les données personnelles proviennent du responsable du traitement et que, par conséquent, le cercle des destinataires n'est pas élargi. D'autre part, selon les circonstances, une personne concernée qui transfère ses données vers le pays dans lequel se trouve le responsable du traitement peut être considérée comme ayant consenti au traitement de ses données dans ce pays, et, dans ce cas, une retransmission des données à partir de ce pays devra également être considérée comme couverte par ce consentement. La question de savoir si le consentement a été donné expressément au sens de la LPD (N 32) est,

bien sûr, une autre question. Il reste à voir si, à l'avenir, les garanties contractuelles seront davantage utilisées lorsque les responsables du traitement se trouvent dans des États tiers qui ne garantissent pas un niveau de protection adéquat des données.

H. Champ d'application de la nLPD

1. Champ d'application personnel

[81] Le champ d'application personnel, matériel et territorial de la LPD n'a pas changé de manière significative – excepté la suppression de la *protection* des données des personnes morales (N 19). Les dispositions pertinentes figurent aux art. 2 et 3 nLPD. Le champ d'application personnel comprend toujours les personnes privées (physiques et morales) et les organes fédéraux. Les organes cantonaux, en revanche, ne sont pas soumis à la LPD ; l'ancienne clause de subsidiarité a même été abandonnée. Les lois cantonales sur la protection des données sont également en cours d'adaptation ou ont déjà été adaptées aux nouvelles exigences du droit européen.

2. Champ d'application matériel

[82] Le champ d'application matériel de la LPD s'écarte encore de celui du RGPD. En principe, la LPD s'applique chaque fois que des données personnelles sont traitées. Les exceptions sont en partie plus étroites et en partie plus larges que dans le cadre du RGPD. Le **traitement manuel des données** n'est couvert par le RGPD que si les données personnelles sont stockées dans un système de fichiers. La LPD ne connaît (toujours) pas cette restriction.

[83] L'exception au champ d'application matériel du traitement des données pour un usage exclusivement personnel est également réglementée différemment. En Suisse, l'exception prévue à l'art. 2 al. 2 let. a nLPD concerne tous les **traitements de données effectués dans le cercle privé de la famille et des amis**. En revanche, l'« exception relative au ménage » prévue à l'art. 2 al. 2 let. c RGPD ne s'applique que si une activité personnelle ou familiale n'a aucun lien avec l'activité professionnelle ou économique de la personne qui traite les données. La LPD ne s'applique pas non plus aux notes personnelles prises à des fins professionnelles, sauf si elles sont partagées avec d'autres personnes. Inversement, le RGPD ne s'applique pas aux échanges purement privés, non professionnels et non commerciaux entre des personnes privées qui ne se connaissent pas – par exemple sur les réseaux sociaux – dans la mesure où ils ne sont pas rendus publics. En Suisse, par contre, la LPD s'applique au *small talk* échangé lors d'une fête avec une personne non apparentée (c'est-à-dire qui n'est ni un ami ni un membre de la famille).

[84] L'exception prévue à l'art. 2 al. 3 nLPD a été entièrement reformulée. Le concept selon lequel le **droit de procédure** applicable devant les tribunaux et les autorités **prime en principe sur la LPD** continue de s'appliquer. Toutefois, les délimitations ont changé. Toutes les lois de procédure fédérales sont couvertes, à l'exception des procédures administratives de première instance (c'est-à-dire les procédures aboutissant à une décision). Il s'agit notamment de la Loi sur la procédure administrative (PA)[66], du Code de procédure civile (CPC)[67], de la Loi fédérale sur la poursuite

66 Loi fédérale sur la procédure administrative (PA) du 20 décembre 1968, RS 172.021.

67 Code de procédure civile (CPC) du 19 décembre 2008, RS 272.

pour dettes et la faillite (LP)[68], du Code de procédure pénale (CPP)[69] et de la Loi sur l'entraide internationale en matière pénale (EIMP)[70]. Les dispositions procédurales applicables aux procédures devant les autorités de conciliation et le juge conciliateur, telles que le juge de paix au sens de l'art. 3 CPC, priment également sur la LPD. Il en va de même depuis peu pour les **tribunaux arbitraux privés** qui ont leur siège en Suisse[71], pour autant qu'ils suivent les règles de procédure fédérales[72]. Du point de vue de la protection des données, cela soulève quelques questions dans la mesure où les règles de procédure concernées ne régissent pas vraiment la protection des données[73] ; celle-ci est largement laissée aux parties ou aux règlements d'arbitrage. Le RGPD ne prévoit pas d'exception similaire pour les tribunaux arbitraux, raison pour laquelle le RGPD s'applique aux arbitres et aux parties ayant un établissement dans l'EEE devant les tribunaux arbitraux suisses.

[85] Selon la LPD actuelle, le champ d'application matériel prend fin lorsque les procédures correspondantes sont en cours, ce qui a entraîné à plusieurs reprises des difficultés de délimitation dans le passé. Désormais, l'accent est plutôt mis sur la question de savoir si un certain traitement de données a lieu « dans » une procédure. C'est le cas si le traitement des données a un lien direct et fonctionnel avec la procédure[74]. En d'autres termes, il doit s'agir d'un traitement de données qui sert la procédure concernée, qui lui est directement lié ou qui est prévu par le règlement de procédure. Cela comprend, par exemple, les mémoires des parties (y compris leur transmission à une autre partie), les déclarations des parties et des témoins et leur traitement, le traitement des preuves recueillies, leur obtention par l'autorité, ainsi que la rédaction et la notification d'une ordonnance ou d'une décision. En revanche, il n'y aura généralement pas de lien direct et fonctionnel dans le cas de recherches et de travaux préparatoires à une procédure. De même, il n'y aura généralement pas de lien direct et fonctionnel lorsqu'une partie envoie à l'avance un projet de mémoire à la partie adverse ou dans les cas de rapports et d'évaluations internes et externes, de communiqués de presse et de couverture médiatique.

[86] L'affirmation dans le message du Conseil fédéral selon laquelle l'exception devrait s'appliquer dès qu'un tribunal ou une autorité est saisie d'une affaire pour la première fois[75] ne va pas assez loin. Le facteur décisif devrait être le **moment** où les règles de procédure sont censées s'appliquer. Le CPC, par exemple, régit déjà le dépôt d'une demande[76] et le CPP la déclaration d'une infraction pénale[77]. Seuls les traitements de données qui ont un lien direct et fonctionnel avec la procédure sont exclus du champ d'application de la LPD.

68 Loi fédérale sur la poursuite pour dettes et la faillite (LP) du 11 avril 1889, RS 281.1.

69 Code de procédure pénale suisse (Code de procédure pénale, CPP) du 5 octobre 2007, RS 312.0.

70 Loi fédérale sur l'entraide internationale en matière pénale (Loi sur l'entraide pénale internationale, EIMP) du 20 mars 1981, RS 351.1.

71 FF 2017 6634.

72 Par exemple, les tribunaux arbitraux internationaux dont le siège est établi conformément au chapitre 12 LDIP.

73 Sur l'ensemble du sujet : David Rosenthal, Complying with the General Data Protection Regulation (GDPR) in International Arbitration – Practical Guidance, in : ASA Bulletin December 2019 No. 4, Kluwer Law International (http://www.rosenthal.ch/downloads/Rosenthal-ArbitrationGDRP.pdf (état au 9 mars 2021)).

74 FF 2017 6634.

75 FF 2017 6634.

76 Art. 130 ss CPC.

77 Art. 309 CPP.

[87] Dans la pratique, ces distinctions seront particulièrement pertinentes pour l'exercice du **droit d'accès**. Si un traitement des données n'est pas couvert par le règlement de procédure, il sera soumis à la LPD (y compris en ce qui concerne le droit d'accès) et indépendamment de l'existence d'une procédure en cours. En revanche, si le droit d'accès doit être utilisé pour obtenir des preuves afin de faire valoir des droits à titre préventif dans le cadre d'une procédure civile, le responsable du traitement pourra soumettre la personne concernée au droit procédural, car les preuves à futur constituent un traitement de données régi par le CPC[78]. Le fait que la procédure ne soit pas encore pendante à ce moment-là n'est plus pertinent dans le cadre de la nLPD.

3. Champ d'application territorial

[88] Le champ d'application territorial est en partie réglementé par l'art. 3 nLPD. Cette disposition est nouvelle, mais ne fait qu'énoncer ce qui est déjà applicable. Le libellé de l'art. 3 al. 1 nLPD correspond à la disposition introduite précédemment dans la loi sur les cartels et précise que le **principe de l'effet**, en tant que concrétisation particulière du principe de territorialité, s'applique également à la LPD. Cet article prévoit en outre que les dispositions de droit public de la LPD s'appliquent à tous les états de fait qui, bien que se produisant à l'étranger, ont ou auront également un impact suffisant sur le territoire suisse. Le Tribunal fédéral a, par exemple, appliqué le principe de l'effet dans l'arrêt « Street View »[79]. Notre Haute Cour n'a toutefois pas dégagé de critère permettant de définir ce que constitue un degré suffisant à l'occasion de cette jurisprudence. Il doit raisonnablement s'agir d'effets perceptibles qui vont au-delà des cas individuels. Par « effet », on entend une atteinte potentielle ou réelle à la personnalité d'une personne concernée en Suisse.

[89] Bien qu'il ne soit pas mentionné, le **principe de territorialité** de la LPD s'applique également dans ses autres aspects : si une partie pertinente des faits soumis à une disposition de droit public de la LPD (p. ex. le traitement de données personnelles, la violation de la sécurité des données) a lieu en Suisse, la disposition de droit public régissant ces faits s'applique, le cas échéant. Il n'est pas nécessaire que l'ensemble des faits aient lieu en Suisse ; un seul acte pertinent en Suisse (comme l'exploitation d'un serveur, la collecte de données, mais aussi les actes déterminant ou favorisant le traitement des données, comme la détermination de la finalité et des moyens essentiels) peut suffire, même si le traitement des données a autrement lieu à l'étranger ou si le responsable du traitement est situé à l'étranger. Si le lieu d'action effectif d'un responsable du traitement ou d'un sous-traitant ne peut être déterminé, on utilisera généralement le siège social ou le lieu de résidence de la personne concernée (au sens d'un **lieu d'action normatif**). Dans le cas des succursales, cependant, le principe de territorialité ne s'applique que s'il existe un lien avec la succursale et que le traitement de données n'est pas effectué à l'endroit de la succursale principale. En cas de traitement de données par la succursale, celle-ci sera dans tous les cas considérée comme un responsable indépendant du traitement. La nLPD continue donc de s'appliquer de manière **extraterritoriale** dès lors qu'un rattachement suffisant avec la Suisse peut être établi, ne serait-ce que parce que les personnes concernées se trouvent en Suisse et qu'un effet pertinent se produit donc en Suisse, même si le traitement des données a lieu à l'étranger et que le respon-

78 Art. 158 CPC.

79 ATF 138 II 346, c. 3.3.

sable du traitement n'a pas son siège en Suisse. La disposition de l'art. 3 al. 1 nLPD va donc plus loin que l'art. 3 al. 2 RGPD.

[90] Les **dispositions de droit public** comprennent, par exemple, le devoir d'informer (art. 19 nLPD), l'obligation de tenir un registre des activités de traitement (art. 12 nLPD), le devoir de procéder à une analyse d'impact relative à la protection des données dans certains cas (art. 22 ss nLPD) et l'obligation d'annoncer les violations de la sécurité des données (art. 24 nLPD). La compétence de surveillance du PFPDT est également de droit public, de même que l'obligation de certains responsables du traitement étrangers de désigner un représentant en Suisse (art. 14 ss nLPD).

[91] En revanche, les principes de traitement (art. 6 et 8 nLPD), la réglementation relative à la sous-traitance (art. 9 nLPD), le droit d'accès (art. 25 ss nLPD) et la réglementation relative à l'atteinte à la personnalité et à sa justification (art. 30 ss nLPD) sont de **nature privée.** Comme par le passé, ces dispositions sont soumises au droit international privé, ce qui est désormais expressément énoncé à l'art. 3 al. 2 nLPD. S'il est possible d'établir un for en Suisse[80], la personne concernée peut choisir le droit applicable au cas d'espèce[81]. Si la personne concernée ou la partie adverse se trouve en Suisse, il faut s'attendre à ce que la LPD s'applique, même si le traitement des données a lieu à l'étranger.

III. Droits des personnes concernées

A. Devoir d'informer et décisions individuelles automatisées

1. Vue d'ensemble

[92] Le devoir d'informer est considérablement élargi dans la nLPD, du moins pour les responsables du traitement qui sont des personnes privées. Alors qu'auparavant les responsables du traitement ne devaient informer la personne concernée que s'ils « collectaient » des données sensibles ou des profils de la personnalité, l'art. 19 nLPD leur impose désormais l'obligation d'informer ***chaque fois*** **que des données personnelles sont collectées**, sauf si l'une des exceptions prévues à l'art. 20 nLPD s'applique. Le contenu du devoir d'informer a également été étendu. En revanche, le devoir d'informer a été réduit pour les organes fédéraux, bien que cela soit probablement dû à un oubli du législateur. D'un point de vue dogmatique, le devoir d'informer est une disposition de droit public, c'est pourquoi sa violation ne constitue pas en soi une atteinte à la personnalité et ne peut donc *pas* être justifiée par l'art. 31 nLPD (motifs justificatifs). La violation intentionnelle est punie d'une **amende** pouvant aller jusqu'à CHF 250'000. Toutefois, seule la personne concernée peut déposer plainte, et non pas le PFPDT. Ce dernier peut tout de même ordonner la transmission d'informations conformes au droit (mais pas l'interruption du traitement des données en raison de l'absence d'informations exigées par l'art. 19 nLPD). Si le PFPDT souhaite mettre fin au traitement des données, il doit le justifier en invoquant une violation de l'obligation de transparence prévue à l'art. 6 nLPD, applicable parallèlement au devoir d'informer. C'est également le sens et le but de l'art. 19 nLPD : il garantit qu'une personne concernée ait accès à des informations *supplémentaires* sur le traitement des données si elle y est intéressée,

80 Art. 129 LDIP, Art. 5 al. 3 Clug.

81 Art. 139 LDIP.

tandis que l'art. 6 nLPD garantit une « transparence de base » qui doit bénéficier de façon générale à toutes les personnes concernées. Le RGPD fait également cette distinction : la transparence de base est régie par l'art. 5 RGPD, alors que le devoir d'informer est prévu aux art. 13 ss RGPD. Cependant, à quelques exceptions près, l'art. 19 nLPD va moins loin que les art. 13 ss RGPD.

[93] Le devoir d'informer en vertu de l'art. 19 nLPD ne s'applique que si le responsable du traitement « collecte » des données personnelles. Cela nécessite **une forme de planification**. Dès lors que le responsable du traitement collecte involontairement ou accidentellement des données personnelles, il n'y a pas d'obligation d'informer. Sont par exemple planifiées la collecte par l'employeur de données relatives aux ressources humaines concernant ses employés, la collecte par le concessionnaire de coordonnées et du détail des transactions de ses clients ainsi que de leurs demandes diverses, ou encore la collecte par la société anonyme des données requises de ses actionnaires de par la loi. Ne sont en revanche pas planifiées la réception occasionnelle d'une demande de renseignements d'un journaliste, le fait de recevoir une carte de visite lors d'une réunion ou encore des signatures figurant au bas de contrats entre entreprises. Par conséquent, il suffit de fournir des informations sur le traitement des données tel qu'il a été prévu par le responsable au **moment de la collecte**. Là encore, les informations doivent avoir été fournies au plus tard à ce moment-là, mais elles peuvent également être fournies à l'avance pour autant que les personnes concernées soient en mesure d'établir un lien entre ces informations et la collecte de leurs données personnelles ; dans le cas d'une collecte indirecte, une réglementation un peu moins stricte s'applique (N 96). Étant donné que l'information est liée à la collecte de données personnelles, il n'est pas nécessaire, lorsque la nLPD entrera en force, d'informer de manière proactive les clients existants, comme cela a parfois été le cas lors de l'entrée en vigueur du RGPD. Il suffit qu'ils soient informés au moment de la prochaine collecte de données (p. ex. au prochain achat, à la prochaine notification de sinistre, etc.) et que la déclaration de protection des données soit par ailleurs disponible sur le site Internet de l'entreprise et référencée dans les brochures, les formulaires, les conditions générales, etc.

[94] Il n'est pas nécessaire d'informer des **modifications ultérieures** (p. ex. le changement du lieu de stockage des données ou l'ajout de catégories de destinataires). Il existe une seule exception à cette règle, à savoir le cas où le responsable du traitement veut utiliser les données collectées (ou obtenues d'une autre manière) dans une finalité supplémentaire. Bien que le RGPD réglemente expressément ce cas, l'art. 19 nLPD ne le fait pas. Ce cas de figure doit être qualifié dans la LPD de manière dogmatique comme une nouvelle collecte de données par le responsable du traitement, même si elle n'est effectuée par ce dernier qu'au moyen de ses propres bases de données et non plus auprès de la personne concernée. Une déclaration de protection des données relativement large, qui prévoit de telles finalités et traitements futurs possibles, est également autorisée même si elle fait référence à des finalités qui ne sont pas encore planifiées.

2. Contenu de l'information

[95] Alors que les art. 13 ss RGPD exigent que la personne concernée soit informée selon le « principe de l'arrosoir », les informations minimales à fournir en vertu de l'art. 19 nLPD sont relativement peu nombreuses. Dans la plupart des cas, la communication de ces informations minimales sera également suffisante. Il faut tout d'abord transmettre l'identité et les coordonnées du responsable du traitement (avec une possibilité de contact par voies postale et électronique ou téléphonique). S'il y a plusieurs responsables conjoints du traitement, il suffit en général de

communiquer l'identité et les coordonnées de l'un d'entre eux (celui auprès de qui les personnes concernées doivent s'adresser ; il doit alors cas échéant en informer les autres responsables du traitement). En outre, les coordonnées d'un éventuel conseiller à la protection des données (au sens de l'art. 10 nLPD) doivent également être fournies, de même que celles de son représentant en Suisse (au sens de l'art. 14 nLPD), si ce dernier a effectivement dû être nommé. Cela n'est toutefois pas réglementé par l'art. 19 nLPD, mais par les dispositions susmentionnées. Les finalités du traitement doivent être indiquées, ce qui permet, contrairement au RGPD, d'utiliser des descriptions brèves telles que « marketing direct », « développement de produits » ou « lutte contre la fraude ». Plus la finalité est définie de manière concise, plus le risque est grand pour le responsable du traitement que cette finalité de traitement soit interprétée de manière restrictive conformément au principe de confiance s'agissant des clauses ambigües.

[96] Les *catégories* de destinataires doivent également être indiquées, bien qu'il soit bien sûr également permis (mais pas obligatoire) de nommer les *différents destinataires*. Les destinataires comprennent non seulement les « tiers », mais aussi tout autre responsable conjoint ou sous-traitant, mais pas les employés, les succursales ou les autres services de l'entreprise. Si une **communication à l'étranger** est prévue – y compris le stockage de données sur des systèmes étrangers (cloud) – il faut indiquer de quels pays il s'agit, qu'ils offrent ou non une protection adéquate des données. Ici, la LPD va plus loin que le RGPD. Toutefois, des indications telles que « tous les pays du monde », « dans le monde entier », « en Europe » ou encore « tous les pays dans lesquels nous sommes représentés » suffisent, car ces pays peuvent être identifiés. Il est également nécessaire d'indiquer quelles garanties de protection des données sont utilisées pour le transfert des données à l'étranger (p. ex. les clauses contractuelles types de l'UE) ou, le cas échéant, à quelles exceptions de l'art. 17 nLPD se réfère le responsable du traitement ; ici aussi, la LPD s'écarte du RGPD. Enfin, des informations doivent également être fournies concernant les décisions individuelles automatisées (cf. N 106 ss).

[97] Lorsque les données ne sont **pas collectées directement auprès de la personne concernée** (ce qui inclut la collecte « interne » de données, p. ex. pour un usage secondaire, mais pas l'observation directe du comportement de la personne concernée, même si celle-ci n'en a pas connaissance), les catégories de données personnelles collectées doivent également être indiquées. Cette obligation ne concerne pas les données générées par le traitement lui-même. La personne concernée doit être informée de la collecte des données dès que le responsable du traitement communique ses données personnelles à des destinataires (même si ce n'est qu'à un sous-traitant ou à un autre responsable conjoint du traitement), mais au plus tard un mois après la collecte.

[98] Ce n'est que dans des cas exceptionnels qu'il sera nécessaire de fournir des **informations plus détaillées** que ces informations minimales, telles que la durée du traitement des données, la source des données, le fondement juridique, un destinataire spécifique ou les droits de la personne concernée. Pour ce faire, l'art. 19 al. 2 nLPD contient une clause générale qui vise à couvrir les cas dans lesquels, en raison de circonstances particulières, tel qu'un risque très élevé d'atteinte à la personnalité, des informations complémentaires sont nécessaires pour évaluer ce risque ou pour garantir l'exercice des droits des personnes concernées. A titre d'exemple pour ce dernier cas de figure, une agence de crédit pourrait expliquer à la personne concernée comment elle peut obtenir des informations de sa part et corriger des données incorrectes (ce qui n'est normalement pas nécessaire, contrairement au RGPD). Il est possible de faire abstraction des informations supplémentaires qui n'intéressent généralement pas les personnes concernées. Par ailleurs, ces infor-

mations supplémentaires ne devront généralement pas aller au-delà de ce qui est requis en vertu des art. 13 ss RGPD.

3. Forme de l'information

[99] L'art. 19 nLPD ne prévoit pas d'**exigence formelle** pour la communication d'informations. En pratique cependant, elle prendra généralement la forme d'une déclaration de protection des données. Des enregistrements audios ou des pictogrammes peuvent également être utilisés[82]. Une **déclaration de protection des données à plusieurs niveaux** (c'est-à-dire d'abord une information brève, puis, à un niveau supérieur, l'information complète) peut être pratique, mais dans la plupart des cas elle n'est pas nécessaire. En droit suisse, il suffit généralement que le responsable du traitement indique à la personne concernée comment obtenir la déclaration de protection des données, à condition que l'on puisse raisonnablement s'attendre à ce qu'elle la consulte. Il n'est *pas* suffisant de se référer à une personne de contact pour toutes questions complémentaires. Par ailleurs, il est n'est pas nécessaire que la personne concernée consulte effectivement la déclaration de protection des données. L'art. 19 nLPD exige seulement que cette dernière soit mise à sa disposition.

[100] Contrairement aux exigences de certaines autorités de protection des données soumises au RGPD, la LPD ne prévoit pas d'« informations de base » qui devraient absolument être fournies au premier niveau d'une déclaration de protection des données à plusieurs niveaux (p. ex. quelles informations devraient être fournies sur un panneau informant sur la vidéosurveillance en plus du lien vers la déclaration de protection des données). Dans les conditions générales ou dans d'autres documents, il suffit généralement de faire référence à la déclaration de protection des données en fournissant un **lien Internet**. Cela entraîne ainsi parfois la nécessité pour la personne concernée de changer de support si elle veut consulter cette information. Toutefois, dans la plupart des cas, au vu de la facilité d'accès à Internet, il est raisonnable d'attendre de la personne concernée qu'elle y consulte la déclaration de protection des données, si elle est intéressée par les informations supplémentaires de l'art. 19 nLPD[83]. L'intérêt de la personne concernée à l'information doit également être pris en compte : si elle peut s'attendre à trouver un lien pour accéder à la déclaration de protection des données dans des documents contractuels, cela n'est toutefois pas le cas sur des cartes de visite, sur le papier en-tête ou au bas de courriers électroniques. Si exceptionnellement une personne concernée est intéressée à accéder à ces informations, on peut s'attendre à ce qu'elle consulte le site Internet de l'entreprise. C'est pourquoi, en vertu de la LPD, il ne sera pas nécessaire de se référer à la déclaration de protection des données dans la vie courante – comme lors de la prise de rendez-vous, à un guichet ou lors d'une réunion. Inversement, cela signifie également que les entreprises doivent rendre leur déclaration de protection des données facilement accessible et reconnaissable sur leur site Internet.

82 Cf. par exemple l'initiative « privacy-icons.ch » du monde des affaires suisse.

83 Après tout, la Suisse estime aussi que ses citoyens ont, par exemple, la possibilité de consulter les lois fédérales s'ils le désirent. Ces informations officielles, et bien d'autres encore, sont aujourd'hui rapidement et facilement accessibles sur Internet. Relevons que la suppression du devoir d'information prévu à l'art. 20 al. 1 let. b LPD se justifie par le fait que les informations nécessaires découlent déjà de la loi – et sont consultables sur Internet par les personnes concernées. Si le législateur attend de ces personnes qu'elles fassent cet effort, la mise à disposition des déclarations de protection des données sur Internet devrait partant également être suffisant.

[101] En ce qui concerne la **formulation** d'une déclaration de protection des données, les mêmes principes s'appliqueront que pour les conditions générales : toute ambiguïté sera interprétée en défaveur de l'auteur. Ainsi, si la signification du terme « marketing direct » n'est pas claire, il sera interprété de manière restrictive. Toute personne souhaitant s'engager dans des formes particulières de marketing direct devra donc les formuler de manière plus explicite. Il convient de signaler expressément les dispositions inhabituelles. Cela résulte toutefois également du principe de transparence prévu à l'art. 6 nLPD.

4. Exceptions

[102] L'art. 20 nLPD définit un catalogue d'**exceptions au devoir d'informer** qui va au-delà de celui prévu par le RGPD. Toute personne invoquant une exception n'est pas tenue de la divulguer. En outre, une personne concernée n'a pas à être informée de ce qu'elle sait déjà. Cela signifie qu'un responsable du traitement n'est pas tenu d'informer chaque fois qu'il collecte des données, s'il existe un certain lien temporel et de contenu entre les informations fournies précédemment et la collecte en cours. Selon le message du Conseil fédéral, les personnes qui mettent leurs données personnelles à la disposition du responsable du traitement sans son intervention sont également considérées comme informées[84]. Si l'on pousse ce raisonnement un peu plus loin, cela signifie que lorsque les circonstances indiquent que la personne concernée a renoncé à l'information en vertu de l'art. 19 nLPD ou n'est pas intéressée par cette information, elle n'a plus besoin d'être informée. Cette approche est parfaitement logique et s'avère même en partie valide sous l'angle du RGPD[85].

[103] Il n'est pas non plus nécessaire d'être informé d'un **traitement prévu par la loi**. La nouvelle exception à l'art. 20 al. 1 let. b nLPD signifie que le devoir d'informer n'est plus requis dans pratiquement tous les cas de traitements de données effectués par les organes fédéraux, ce qui est surprenant. D'ailleurs, les responsables du traitement qui sont des personnes privées bénéficient également de cette exception dans la mesure où une disposition de droit suisse prescrit le traitement des données. C'est le cas non seulement pour les obligations instituées par des lois spéciales, telles que celles relatives à la lutte contre le blanchiment d'argent, mais également pour le traitement de données au quotidien, comme la comptabilité ou la tenue d'un dossier du personnel (ou des dossiers d'une étude d'avocats). Cette exception au devoir d'informer sur la base d'une obligation légale de traitement des données correspond d'ailleurs à la pratique actuelle du PFPDT relative à l'obligation de déclarer les fichiers[86]. Cela ne s'applique pas aux dossiers du personnel, même selon la pratique actuelle.

[104] D'autres exceptions prévues à l'art. 20 nLPD se fondent sur le secret professionnel et la protection des sources des professionnels des médias. En cas d'obtention indirecte de données, il peut être renoncé à l'information si le responsable du traitement ne peut pas informer la personne concernée parce qu'il ne pourrait l'identifier et la localiser qu'au prix d'**efforts disproportionnés**

84 FF 2017 6671.

85 En effet, l'art. 32 § 1 BDSG, qui complète le RGPD en l'Allemagne, prévoit qu'il est possible de renoncer à l'information dans le cas de données stockées de manière analogue lorsque l'intérêt de la personne concernée à recevoir cette information doit « être considéré comme minime » au vu des circonstances.

86 Art. 11a LPD.

(dans la mesure où cela est nécessaire pour l'informer)[87] ou que les efforts requis pour l'informer seraient eux-mêmes disproportionnés. La proportionnalité est évaluée sur la base de l'importance de l'effort exigé du responsable du traitement par rapport à l'importance de l'intérêt de la personne concernée à l'information. L'intérêt de la personne concernée à exercer ses droits vis-à-vis du responsable du traitement est inclus dans cette évaluation. Toutefois, en cas de pluralité de personnes concernées, des considérations individuelles ne sont pas nécessaires ; elles peuvent être objectivées et généralisées.

[105] Enfin, l'art. 20 al. 3 nLPD prévoit que le devoir d'informer peut être partiellement ou entièrement suspendu ou reporté sur la base d'une **pesée des intérêts**. C'est le cas, d'une part, si l'information porte atteinte aux intérêts de tiers (p. ex. parce que l'information elle-même contient des données personnelles de tiers ou porte atteinte à l'intérêt de tiers au maintien du secret) et, d'autre part, si l'information compromet sérieusement la réalisation de l'objectif poursuivi par le traitement des données et que cet objectif semble plus important que le fait d'informer (immédiatement) la personne concernée (p. ex. parce qu'un devoir d'informer au préalable de la surveillance par un détective privé irait à l'encontre du but de la surveillance). Un responsable du traitement peut invoquer des intérêts privés prépondérants (p. ex. l'intérêt au maintien du secret) dans la mesure où il ne prévoit pas de communiquer les données personnelles à des tiers (ce qui inclut d'autres responsables du traitement indépendants – y compris les autorités – mais pas les responsables du traitement conjoints, les sous-traitants ou encore – en cas de règlementation expresse – les sociétés d'un même groupe). Les organes fédéraux peuvent restreindre l'information sur la base d'intérêts publics prépondérants ou en lien avec le déroulement d'une procédure, bien qu'ils ne soient de toute façon généralement pas tenus d'informer en vertu de leurs obligations légales (et de la primauté du droit procédural prévue à l'art. 2 nLPD).

5. Décisions individuelles automatisées

[106] La réglementation des décisions individuelles automatisées prévue à l'art. 21 nLPD est nouvelle en Suisse ; dans le reste de l'Europe, elle existe depuis un certain temps, mais dans la pratique, elle a joué jusqu'à présent un rôle secondaire. Au vu de l'accroissement actuel des gros titres sur l'utilisation de l'« intelligence artificielle » (IA), elle s'inscrit certainement dans la tendance. Elle repose sur l'idée que les machines ne doivent pas prendre de décision concernant les individus, du moins pas lorsqu'il s'agit de décisions importantes. Ce n'est pas en soi une question de protection des données, mais elle est réglementée ici car toute décision de ce type repose en fin de compte sur un processus logique, dont le problème réside dans l'imperfection du traitement des données nécessaire à la décision.

[107] Comme dans le cas du profilage, et contrairement à son libellé qui peut sembler large, l'expression « décisions individuelles automatisées » ne désigne en définitive que les décisions pour lesquelles une machine dispose d'un *pouvoir d'appréciation*[88]. La machine prend une décision sur la base d'une évaluation des données personnelles à sa disposition, que la machine les ait « apprises » ou qu'un être humain les ait programmées. Par exemple, la machine évalue si le relevé de

87 La disposition fait référence à ce cas lorsqu'elle indique que l'information est « impossible » à donner.

88 A l'inverse, le message du Conseil fédéral considère que les décisions « simples » ne sont pas couvertes par le terme (FF 2017 6674). À titre d'exemple de décision « simples », il cite la décision du distributeur automatique de remettre l'argent si le solde du compte est suffisant.

notes d'un candidat présente une moyenne suffisante pour accéder au prochain tour du processus ; ou si le client d'une banque bénéficie exceptionnellement d'une autorisation de découvert, bien que cela n'ait pas été convenu. La « non-valeur » réside ici dans le fait que la machine sera limitée par les données et les coefficients qui ont été programmés ou – dans le cas d'une IA – appris. Mais il ne s'agira jamais de *toutes* les circonstances. Si, en revanche, une personne (parfaite) devait juger le même candidat, elle lui donnerait probablement une chance malgré ses notes peu convaincantes, car un autre aspect de sa candidature justifierait exceptionnellement un traitement particulier. Il n'est pas question ici de savoir si l'hypothèse du législateur est correcte, à savoir que les humains prennent de meilleures décisions discrétionnaires et, à l'inverse, que les machines suivent « aveuglément » n'importe quelles instructions lorsqu'elles prennent des décisions. Quoi qu'il en soit, ce point de vue est à l'origine de la réglementation.

[108] Par conséquent, seules les décisions qui sont **entièrement prises par une machine** et qui supposent un pouvoir d'appréciation sont concernées, c'est-à-dire celles qui requièrent une évaluation ou une interprétation. Le système de contrôle d'accès, qui déverrouille la porte lorsqu'un badge valable est présenté, ne prend aucune décision individuelle automatisée car il n'y a pas de place pour l'interprétation. En outre, aucune décision individuelle automatisée n'est prise s'il existe un accord préalable avec la banque selon lequel le compte bénéficie d'une autorisation de découvert jusqu'à CHF 1000 et si le distributeur automatique de billets applique strictement cette limite[89]. Le distributeur automatique de billets ne prend pas de décision, il en applique simplement une. Si, en revanche, la banque laisse son ordinateur déterminer une limite de découvert individuelle pour chaque client – sur la base de ses entrées et sorties de paiements – il s'agit d'une décision individuelle automatisée. Il n'y a pas de décision individuelle automatisée lorsqu'un ordinateur suggère des limites de découvert individuelles à un employé de banque, mais que celles-ci sont finalement approuvées par l'employé. Du point de vue de la protection des données, il s'agit d'un profilage (l'ordinateur évalue la solvabilité du client concerné de manière entièrement automatique), mais aucune décision n'est prise de manière automatisée (la nLPD s'écarte du RGPD à cet égard[90]). Dans ce contexte, le fait qu'une décision prise par une machine soit communiquée par la machine ou par un être humain (et que l'être humain ne puisse ou ne doive plus influencer la décision) est sans importance.

[109] En outre, toutes les décisions individuelles automatisées ne sont pas concernées, seulement celles qui entraînent une **conséquence juridique** pour la personne concernée ou qui l'**affectent de manière significative**. Une conséquence juridique peut être, par exemple, la conclusion automatique d'un contrat à certaines conditions ou sa résiliation automatique[91]. Si, en revanche, la conclusion d'un contrat est automatiquement rejetée, comme dans l'exemple du candidat, il n'y a *pas* de conséquence juridique, mais la personne concernée – dans cet exemple – peut encore être affectée de manière significative. Dans ce cas, il s'agit de ses intérêts économiques, mais une telle

89 FF 2017 6674.

90 Selon l'art. 22 al. 1 RGPD, le profilage est également considéré comme une décision individuelle automatisée. Toutefois, le Parlement suisse a supprimé cette référence dans le libellé de l'art. 21 al. 1 nLPD au cours des délibérations.

91 FF 2017 6674. Le message du Conseil fédéral affirme de manière erronée que l'envoi automatisé d'une facture n'est pas une décision individuelle automatisée avec des conséquences juridiques, car les *conséquences juridiques* résultent de la conclusion du contrat. Ainsi, il ne s'agit pas d'une décision individuelle au sens strict, dans la mesure où il n'y a pas de pouvoir d'appréciation, car l'ordinateur ne facture de manière automatique que les sommes convenues au préalable, et qui concernent le montant et l'échéance. Toutefois, la décision entraîne des conséquences juridiques.

décision peut également porter atteinte à des intérêts personnels (p. ex. l'attribution automatisée d'une prestation médicale[92]). En revanche, si un ordinateur décide automatiquement quelles publicités sont montrées au visiteur d'un site Internet en fonction de son profil spécifique, ce dernier n'est pas affecté de manière significative. Une simple nuisance ne suffit pas, comme le montre clairement le message du Conseil fédéral[93].

[110] Si un ordinateur ne décide pas du sort d'une seule personne, mais qu'il doit prendre une décision générale (p. ex. quel groupe de clients doit bénéficier d'une réduction ou comment les prix des billets doivent être ajustés sur une base quotidienne en fonction des capacités encore disponibles), il ne s'agit pas non plus d'un cas prévu par l'art. 21 nLPD. Peu importe que la décision individuelle automatisée soit minutieuse ou qu'une personne comprenne pourquoi l'ordinateur a pris cette décision[94]. Les décisions fondées sur le hasard sont tout autant concernées que celles qui reposent sur une évaluation complexe de grandes quantités de données, qu'elles soient programmées par un être humain ou « apprises » par l'ordinateur lui-même.

[111] Lorsqu'une décision individuelle automatisée est prise, elle entraîne deux conséquences juridiques : d'une part, la **personne concernée** doit être **informée** et, d'autre part, cette dernière a le droit, après avoir exposé son point de vue, de faire contrôler la décision par un être humain en chair et en os. La personne concernée a donc **droit à une « audition humaine »**. Contrairement à la disposition correspondante du RGPD, qui n'établit pas clairement si les décisions individuelles automatisées sont en principe interdites ou si elles donnent droit à la personne concernée à un contrôle humain, les décisions individuelles automatisées sont en principe autorisées en Suisse. Toutefois, il convient d'examiner dans des cas concrets si elles sont disproportionnées ou si elles violent d'autres principes généraux régissant le traitement des données, comme par exemple l'exactitude des données.

[112] Cette information peut être fournie lors de la notification de la décision. Toutefois, une information générale figurant au préalable dans une déclaration de protection des données est également valable. Il est essentiel que, dans le cas d'une telle décision, la personne concernée soit mise en mesure de demander un contrôle par un humain et des informations sur la logique de la décision (N 112 ss). Pour ce faire, elle doit au moins savoir **quelles décisions sont prises automatiquement** (le devoir d'informer ne concerne pas toutes les décisions automatisées, mais uniquement celles qui relèvent de l'art. 21 nLPD) et comment elle peut faire valoir son droit à une « audition humaine » (ces informations peuvent également être transmises avec la décision). Des informations supplémentaires ne seront normalement pas nécessaires car la personne concernée dispose déjà de ces informations grâce au droit d'accès (N 115 ss).

[113] Lorsqu'une personne concernée exerce son droit à l'« audition humaine », elle a le droit d'être entendue, y compris sur les aspects que la machine n'a pas pris en compte. Elle doit être entendue par une personne habilitée à annuler la décision. Cependant, cette personne n'est pas obligée d'annuler la décision tant qu'elle **réexamine la décision de bonne foi**. Le responsable du traitement conserve ainsi une certaine liberté dans sa décision. L'art. 21 nLPD ne dit pas dans quel délai il doit accorder une « audition humaine ». Dans de nombreux cas, dix jours dès la notification de la décision suffisent – par analogie au délai de recours prévu dans certains cantons.

92 FF 2017 6674.

93 FF 2017 6674.

94 Comme par exemple les systèmes de reconnaissance de formes qui sont « entraînés » au lieu d'être programmés (appelé aussi *deep learning*).

Le délai est communiqué à l'avantage de la personne concernée. Le droit à une audition humaine peut être satisfait, par exemple, si la décision informe la personne concernée que la décision a été prise par une machine et que, en cas de désaccord, elle peut parler à un représentant du responsable du traitement qui réexaminera la décision après l'avoir entendue.

[114] Si la machine a pris une décision dans le cadre de la conclusion ou de l'exécution d'un contrat **conformément à ce que la personne exigeait**, aucun réexamen ne peut être demandé (art. 21 al. 3 let. a nLPD, qui s'écarte de ce qui est prévu par le RGPD). Mais surtout, la personne n'a pas à en être informée, c'est-à-dire qu'à l'inverse il suffit de l'en informer en cas de décision négative (sauf si elle a déjà été informée du processus de décision automatisé dans la déclaration de protection des données). Une boutique en ligne qui conclut automatiquement des contrats prend généralement des décisions individuelles automatisées[95], mais elle ne doit proposer un réexamen que si elle rejette automatiquement la commande, ce qui a peu de chances de se produire. Selon l'art. 21 al. 3 let. b nLPD, une personne peut également **renoncer** par avance au droit à un réexamen en acceptant expressément une décision automatisée (p. ex. parce que de telles décisions sont régulièrement prises dans le cadre d'une relation contractuelle). Dans ce cas, cependant, au vu de l'exigence de consentement éclairé, il faudra en principe faire en sorte que la personne soit informée de ce à quoi elle renonce, soit à l'audition humaine. Sans cette information, la renonciation de la personne concernée ne sera pas valable.

B. Droit d'accès

1. Vue d'ensemble

[115] Le droit d'accès prévu à l'art. 25 nLPD complète le devoir d'informer des art. 19 ss nLPD. Il est donc structuré de manière similaire. Toutefois, il va plus loin en termes de contenu, c'est-à-dire que la personne concernée peut en apprendre plus par ce biais que ce que le responsable du traitement doit divulguer dans le cadre de sa déclaration de protection des données. D'un côté, cette nouvelle disposition a été élargie pour inclure certaines informations à fournir, mais d'un autre, elle a également été limitée s'agissant de l'**utilisation abusive** du droit d'accès afin d'obtenir des preuves, qui est une pratique courante aujourd'hui. Lors du processus de consultation, cette question a ainsi également été un sujet de préoccupation majeur[96]. Par ailleurs, le droit d'accès n'est plus limité à la collecte de données, bien que cela soit d'une importance secondaire dans la pratique : dans l'UE, cette restriction n'a jamais existé ; en Suisse, les demandes d'accès ont rarement été refusées pour cette raison. En dehors de cela, le droit d'accès révisé correspond pour l'essentiel au droit actuel[97]. Il s'agit d'un droit strictement personnel auquel on ne peut pas renoncer à l'avance (art. 25 al. 5 nLPD). Une personne capable de discernement peut et doit l'exercer elle-même (ou un représentant légal agissant en son nom) ; pour les enfants incapables de discernement, cela peut être fait par leur représentant légal (p. ex. les parents qui veulent vérifier si les données de leurs enfants sont traitées correctement par la crèche).

95 Dans la mesure où la commande du client est considérée comme une offre contractuelle selon le droit des obligations, qui doit encore être acceptée par le commerçant.

96 FF 2017 6683.

97 FF 2017 6683.

[116] Certaines violations du droit d'accès peuvent faire l'objet de **sanctions pénales**. Toutefois, elles doivent être intentionnelles. En pratique, la personne qui risque l'amende est celle qui décide d'accorder l'accès ou non. Il peut également s'agir d'un employé. Toutefois, la personne qui fournit des informations n'est sanctionnée que si elle fournit intentionnellement des informations fausses ou incomplètes, comme la LPD le prévoyait jusqu'à présent, ou si elle ne réagit pas du tout, ce qui est une nouveauté. Celui qui répond à la demande mais prétend, à tort ou à raison, ne pas être tenu de fournir des renseignements n'est pas punissable, car la personne concernée peut intenter une action civile si nécessaire[98]. De même, une information incomplète n'est punissable que si elle donne intentionnellement l'impression d'être complète[99]. Comme il n'existe pas d'obligation de fournir une déclaration d'intégralité, il est judicieux de s'en abstenir.

2. Contenu, forme et moment de l'accès

[117] Le droit d'accès permet en substance à toute personne physique d'exiger que le responsable du traitement lui indique **s'il traite des données personnelles la concernant et, dans l'affirmative, lesquelles**. En outre, le responsable du traitement doit – sur demande – fournir les informations énumérées à l'art. 25 al. 2 nLPD. Celles-ci ont été calquées sur le RGPD : informations relatives à l'identité du responsable du traitement, à la finalité du traitement, à la durée de conservation (ou à ses critères), à la source des données (si elle est disponible), aux décisions individuelles automatisées (et à la logique sur laquelle elles se fondent), aux catégories de destinataires (p. ex. les autorités ou les sociétés d'un groupe, sans nécessité de donner les noms), et aux informations sur l'exportation conformément à l'art. 19 al. 4 nLPD (N 95)[100]. Certaines informations moins pertinentes ont été supprimées (base légale, catégories de données personnelles, participants au fichier). Cela correspond aux exigences du RGPD, à l'exception des informations qui y sont toujours requises concernant les droits des personnes concernées et le droit de recours. Les informations relatives à l'exportation de données diffèrent en termes de contenu de celles requises par le RGPD.

[118] Parmi les informations supplémentaires, celles relatives à l'identité du responsable du traitement et à la durée de conservation seront particulièrement difficiles à communiquer en pratique, même si aucune information spécifique n'est requise à cet égard et qu'il n'est pas nécessaire de mentionner toutes les exceptions. Aujourd'hui, la plupart des déclarations de confidentialité « esquivent » les explications claires sur ces points, bien que le RGPD lui-même les exige. En ce qui concerne l'**identité du responsable du traitement,** le principal problème réside dans le fait que, dans de nombreux cas, la partie qui fournit les informations ne sait pas du tout clairement qui, en dehors du responsable du traitement « principal », doit être considéré comme responsable (conjoint) du traitement. Il n'est même pas nécessaire de les indiquer dans la déclaration de protection des données (N 99 ss). Dans le cadre du droit d'accès, les responsables du traitement doivent être désignés si une raison particulière le justifie, par exemple parce que le responsable principal est à l'étranger et que la personne concernée souhaite avoir affaire à un (éventuel) co-

98 FF 2017 6716.

99 FF 2017 6716.

100 *[La version allemande]* du texte du vote final contient ici une erreur rédactionnelle qui sera probablement corrigée dans le texte final : la référence à l'« article 19 » a été supprimée par inadvertance. *[Cette référence figure toutefois dans la version française du texte.]*

responsable en Suisse afin de pouvoir exercer plus facilement ses droits. C'est là qu'intervient la **clause générale** de l'art. 25 al. 2 nLPD, qui va au-delà de ce que prévoit le RGPD : si cela est nécessaire pour faire valoir ses droits en matière de protection des données, la personne concernée peut également demander des informations complémentaires qui ne sont *pas* énumérées à l'al. 2[101]. Il pourrait s'agir, par exemple, de savoir où les personnes concernées peuvent faire valoir certains droits ou qui a reçu certaines données personnelles[102]. En théorie, il peut également s'agir d'informations que le RGPD n'a pas envisagées, comme par exemple des informations sur des aspects particuliers d'accords avec d'autres responsables du traitement avec qui des données sont échangées. Des informations complémentaires allant au-delà du minimum requis par la loi resteront toutefois l'exception, par analogie avec ce que prévoit l'art. 19 nLPD, et devront être justifiées[103]. Rien n'indique en tout cas qu'avec ce droit d'information étendu le législateur ait voulu introduire par une porte dérobée un droit d'audit pour les personnes concernées ; par ailleurs, la protection contre la divulgation des secrets des responsables du traitement serait alors bien trop insuffisante. De plus, les responsables du traitement ne devront en principe fournir d'information complémentaire qu'en réponse à des demandes précises. Cela correspond à un principe qui s'est également imposé dans la pratique à d'autres situations : la première réponse contiendra ce qui intéresse généralement les personnes concernées. Si elles en veulent plus, elles devront le demander de manière précise[104].

[119] En ce qui concerne les **décisions individuelles automatisées**, il n'est pas nécessaire de fournir des informations détaillées sur la logique sur laquelle elles se sont fondées. Comme cela ressort déjà du RGPD, des informations relativement générales suffisent. Dans le cas d'une évaluation de crédit automatisée, par exemple, il faudrait indiquer qu'elle est basée sur une évaluation de la solvabilité de la partie intéressée et de sa provenance (p. ex. si elle provient d'une agence de crédit) ou sur le type d'informations sur lesquelles la notation est basée et leur pondération (p. ex. des données en matière de poursuites, des antécédents de paiement, etc.)[105]. Des informations doivent également être fournies sur l'existence d'une décision individuelle automatisée en tant que telle. Cela ne signifie toutefois pas qu'une personne physique peut exiger qu'une entreprise publie un catalogue de toutes ses décisions individuelles automatisées. Premièrement, le responsable du traitement ne devra fournir que les informations dont on peut raisonnablement s'attendre à ce qu'elles concernent la personne à l'origine de la demande et, deuxièmement, il peut exiger que cette personne précise les opérations de traitement qui l'intéressent (p. ex. le traitement des demandes de remboursement par une caisse d'assurance maladie). Cette restriction s'applique au droit d'accès en général : dans tous les cas, si un responsable du traitement traite *beaucoup de données sur une personne*, il peut normalement exiger de cette dernière qu'elle **précise**

101 FF 2017 6683.

102 Cf. art. 19 RGPD.

103 Par exemple, en fournissant des preuves concrètes d'une violation de ses droits en matière de protection des données et en expliquant pourquoi elle a besoin de recevoir ces informations complémentaires dans le cadre du droit d'accès afin de pouvoir faire valoir ses droits (et non p. ex. par le biais de l'obtention de preuves dans le cadre d'une procédure civile). Si la personne concernée ne peut pas le faire, l'information n'est pas « nécessaire » au sens de la LPD.

104 Cela s'applique indépendamment de l'expression « dans tous les cas » de l'art. 25 al. 2 nLPD, puisque cet alinéa indique uniquement quelles sont les informations obligatoires qu'une personne concernée peut demander dans tous les cas, sans avoir à expliquer pourquoi elle en a besoin pour faire valoir ses droits en matière de protection des données.

105 FF 2017 6684.

sa demande d'information[106]. Il doit en être de même pour les responsables de traitements qui effectuent *de nombreux traitements de données.* Ces restrictions découlent à l'origine de l'art. 25 nLPD et pas seulement des exceptions de l'art. 26 nLPD.

[120] Les informations nécessaires contiendront naturellement une **liste des données personnelles traitées**. Ici, le Parlement a ajouté cette précision « en tant que telles » à l'art. 25 al. 2 let. c nLPD. Il en ressort de manière claire que ce ne sont pas des documents qui peuvent être demandés mais uniquement des données personnelles. Cela est également conforme à la pratique de la CJUE[107]. Cette clarification est devenue nécessaire car de nombreux tribunaux suisses – y compris le Tribunal fédéral – ont ignoré la règlementation déjà applicable auparavant et ont généreusement donné suite aux demandes de production de documents (p. ex. des emails, des contrats, des rapports)[108] et non pas seulement de données personnelles (p. ex. certains propos concernant une personne contenus dans des emails et des rapports). Il s'agit d'une des raisons de l'abus généralisé du droit d'accès.

[121] Cela conduit à la question de la délimitation d'une donnée personnelle : si une personne a signé un contrat, est-ce que l'ensemble du contrat constitue une donnée personnelle ou seulement sa signature ? Il n'est évidemment pas possible de répondre à cette question de manière générale. En raison de la finalité du droit d'accès (al. 2), le facteur décisif dans ce cas sera la manière dont l'information est utilisée. Si elle n'est pas utilisée comme donnée personnelle de la personne concernée et qu'il n'y a pas de risque majeur que cela se produise, l'information ne sera pas soumise au droit d'accès. Le CEO qui a signé un contrat de son entreprise l'a fait en sa qualité de CEO. En règle générale, il ne lui est pas nécessaire de connaître le contenu du contrat pour faire valoir ses droits en matière de protection des données. L'intégralité du contrat n'a donc pas besoin de lui être communiqué.

[122] En ce sens, la nouvelle règle générale de l'art. 25 al. 2 nLPD limite clairement le droit d'accès : le droit d'accès vise uniquement à aider une personne concernée à faire valoir ses droits en matière de protection des données (au moins ses droits pouvant faire l'objet d'une action en justice) et à garantir la transparence du traitement des données (p. ex. pour permettre à une personne de choisir de fournir ou non des données ou de savoir – pour sa tranquillité d'esprit – quelles données une entreprise détient à son sujet). En revanche, le droit d'accès ne sert pas à obtenir des preuves pour faire valoir d'autres prétentions.

[123] **En principe**, les informations doivent être fournies **gratuitement,** mais le Conseil fédéral prévoira dans l'ordonnance sur la nLPD des exceptions en cas de frais disproportionnés. Jusqu'à présent, les exceptions ne méritaient pas d'être mentionnées. Le Parlement a fixé à 30 jours le délai pour la communication des informations, mais des exceptions sont possibles. Le Conseil fédéral les définira probablement aussi dans l'ordonnance. Il est intéressant de noter que l'art. 25 nLPD ne prévoit plus que les informations doivent être fournies **par écrit**. Le RGPD, en revanche, prévoit que les personnes concernées peuvent demander une copie des données personnelles. Cette nouvelle réglementation pourrait conduire à une situation dans laquelle les responsables

106 FF 2017 6683 avec renvoi au considérant 63 du RGPD.

107 Arrêt de la CJUE du 17 juillet 2014 (C-141/12 et C-372/12), dans lequel la CJUE a estimé que le droit d'accès ne conférait pas de droit à recevoir une copie de l'ensemble d'un document contenant des données personnelles, même si certaines parties de celui-ci sont caviardées. La CJUE interprète également la notion de donnée personnelle de manière étroite. Dans l'affaire en question, une personne concernée a tenté d'obtenir la publication d'un projet de décision.

108 Cf. par exemple l'arrêt du Tribunal fédéral 4A_506/2014 du 3 juillet 2015, En fait B.

du traitement de données sensibles ou nombreuses estimeront que l'accès peut uniquement être accordé sur place. Dans ce cas, le Conseil fédéral ou la jurisprudence devront décider dans quelle mesure des copies devront à l'avenir être faites, même en l'absence de disposition légale expresse.

[124] Dans le cadre de l'obligation de fournir des renseignements, l'**identification** fiable de la personne qui en fait la demande demeure obligatoire (même si elle n'est pas mentionnée à l'art. 25 nLPD), ce qui se fait aujourd'hui généralement au moyen d'une copie de la carte d'identité (mais ce n'est pas obligatoire)[109].

3. Restrictions au droit d'accès

[125] Le législateur a apporté deux modifications principales aux motifs justificatifs permettant de limiter l'obligation de fournir des renseignements prévus par l'art. 26 nLPD. La première modification tente à nouveau de mettre un terme aux abus : selon l'art. 26 al. 1 let. c nLPD, la transmission des renseignements peut être refusée ou du moins restreinte ou différée si la demande est « **manifestement** » **infondée ou procédurière**. Ce dernier cas de figure est probablement le plus simple. Il couvre, entre autres, les demandes d'accès qui servent de toute évidence à nuire au responsable du traitement ou à le solliciter inutilement (p. ex. par des demandes répétées ou en sachant qu'il ne traite aucune donnée nous concernant[110])[111]. Les demandes d'information sont manifestement infondées si elles ne poursuivent pas les objectifs mentionnés à l'art. 25 al. 2 nLPD, c'est-à-dire si elles ne servent pas à faire valoir des droits en matière de protection des données ou à instaurer une certaine transparence dans ce domaine. Le Conseil fédéral a été trop restrictif à cet égard dans son projet de loi en ce sens qu'il a essentiellement confirmé la jurisprudence qui permettait d'exiger une justification à la demande d'accès[112]. Le Parlement a voulu mettre un terme à cette situation : selon l'art. 26 al. 1 let. c nLPD, une demande d'accès est manifestement infondée si elle « poursuit un but contraire à la protection des données »[113]. Il s'agit d'un changement de système : pour présumer un abus, il n'est plus nécessaire de démontrer que la demande d'accès ne poursuit aucun objectif de protection des données (ce qui était impossible en pratique), il suffit de démontrer qu'elle poursuit manifestement un objectif *étranger* à la protection des données. Cela pourrait être le cas, par exemple, si un employé, suite à son licenciement prétendument injustifié, exige de son ancien employeur par l'entremise de son avocat la remise de tous les e-mails et procès-verbaux le concernant : il est évident qu'il tente de justifier des prétentions de droit du travail. A la lumière du nouveau droit, même l'ATF 138 III 425 – cet

109 Selon le RGPD, la demande d'une copie de la carte d'identité peut même constituer une violation de ce règlement lorsqu'une telle demande n'est pas absolument nécessaire.

110 FF 2017 6686.

111 Par exemple des services en ligne qui permettent à un utilisateur d'envoyer des demandes d'accès automatisées et en masse à des entreprises avec lesquelles il n'a jamais eu de contact et pour lesquelles il n'existe aucune preuve qu'elles détiennent ses données personnelles. La nouvelle disposition devrait permettre de rejeter ces demandes d'information en série. Cf. David Rosenthal/David Vasella, Erste Erfahrungen mit der DSGVO, in : Digma, décembre 2018, Numéro 4 (http://www.rosenthal.ch/downloads/digma_2018_4_Rosenthal_Vasella.pdf (état au 9 mars 2021)), p. 169, au sujet de « One.Thing.Less », un fournisseur de demandes d'accès automatisées en Suisse.

112 FF 2017 6685 ss, et les réf. cit.

113 La formulation « contraire à la protection des données » est quelque peu malheureuse, mais compte tenu de la motivation de cet ajout, l'intention du législateur et l'objectif de la disposition semblent clairs. Exiger qu'une demande d'information ne poursuive non seulement pas des fins de protection des données, mais même des fins contraires à la protection des données prive cet ajout de son sens. Une demande d'information serait alors contraire à la protection des données si elle conduisait à la violation de la protection des données d'une autre personne. Cependant, ce cas est déjà couvert par l'art. 26 al. 1 let. b nLPD.

audacieux arrêt de principe du Tribunal fédéral qui a ouvert la voie aux abus en matière de droit d'accès – devrait être réévalué.

[126] La deuxième modification concerne (malheureusement seulement) un allégement pour les groupes de sociétés. La question était de savoir si une personne privée responsable du traitement pouvait toujours restreindre, différer ou refuser la communication de renseignements demandés dans la mesure où ses propres intérêts prépondérants l'exigeaient. Le Conseil national soutenait cette solution au motif qu'elle serait cohérente : si un intérêt est objectivement prépondérant, il n'y a aucune raison de ne pas le respecter. C'est également ce que prévoient d'autres dispositions de la LPD (art. 17 al. 1 let. c ch. 1 nLPD, art. 31 al. 1 nLPD). Cependant, le Conseil des États a réussi à imposer le maintien de la solution qui prévalait jusqu'à maintenant : le responsable du traitement ne peut faire valoir **ses intérêts prépondérants** (p. ex. des secrets d'affaires, des informations concernant la formation d'opinion ou encore des frais excessifs) que lorsqu'il s'agit de données personnelles qu'il ne prévoit pas de communiquer à des tiers. La seule restriction à la règle de l'art. 26 al. 2 nLPD par rapport au droit actuel est la précision à l'al. 3 selon laquelle les autres entreprises du groupe ne sont pas considérées comme des tiers. Jusqu'à présent, les sous-traitants et les responsables conjoints du traitement n'étaient pas non plus considérés comme des tiers. À cet égard, la nLPD est donc plus stricte que le RGPD.

[127] Par exemple, une banque ne peut pas invoquer ses secrets d'affaires (bien que cela soit justifié) lorsqu'elle doit par exemple régulièrement communiquer des données personnelles à la FINMA, car cette dernière est considérée comme un tiers. La décision du Parlement est particulièrement problématique parce que le droit d'accès lui-même n'oblige pas la personne qui en demande l'accès à garder secrète l'information reçue. Il est probable que le Parlement n'ait pas été conscient de ces conséquences et qu'il s'agisse donc d'un oubli. Toutefois, il n'y a probablement rien à redire à ce sujet, étant donné le contexte législatif clair. En pratique, des solutions possibles à ce problème pourraient être que, dans de tels cas, l'accès ne soit accordé que sur place (si l'ordonnance le permet) ou que l'information soit fortement restreinte, conformément à ce que prévoit la loi, de sorte que seules les données personnelles « en tant que telles » soient communiquées. Il est également concevable de considérer qu'il s'agit d'un but contraire à la protection des données lorsque la demande d'accès vise à obtenir des secrets d'affaires.

[128] Comme auparavant, il est toujours possible de restreindre, différer ou refuser de fournir des informations si une obligation légale le prévoit ou si les intérêts prépondérants de tiers l'exigent. C'est tout d'abord le cas lorsque, comme cela est maintenant expressément prévu dans la loi, le refus de fournir des informations demandées est nécessaire pour protéger un **secret professionnel**. Cela peut par exemple être invoqué par l'avocat (même s'il est lui-même responsable du traitement et donc obligé de fournir des informations), mais pas par son client. Le client (p. ex. un groupe d'entreprises) doit faire valoir un intérêt prépondérant qui lui est propre, ce qu'il ne peut faire, comme indiqué plus haut, s'il transmet par exemple ces données à un autre responsable du traitement extérieur au groupe (p. ex. à une autorité ou à un partenaire commercial).

[129] Si le responsable du traitement souhaite invoquer l'une de ces exceptions, il peut exiger de la personne concernée qu'elle démontre son propre **intérêt à accéder à l'information**[114]. En dehors de ce cas de figure, elle n'a pas à justifier sa demande d'information et n'a pas besoin de motif particulier. La curiosité suffit, comme le confirme également le message du Conseil fédé-

114 ATF 138 III 425, c. 5.4 ss ; ATF 123 II 534, c. 2e.

ral[115]. Le responsable du traitement doit, à son tour, justifier les raisons pour lesquelles il refuse, restreint ou diffère la communication des renseignements. En cas de litige, il devra également démontrer en quoi la méthode de « limitation » de l'information qu'il a choisie (p. ex. un caviardage, voire une opposition totale à la communication des renseignements) était la mesure la moins dommageable possible.

C. Droit à la remise et à la transmission des données

[130] Le nouveau **droit à la remise et à la transmission des données** (également appelé droit à la « portabilité des données ») prévu par les art. 28 ss nLPD n'a été introduit que lors des délibérations parlementaires. Il n'existe aucun document officiel à ce sujet. La règlementation est calquée sur celle du RGPD[116]. Il ne s'agit pas de protection des données au sens strict, mais plutôt de **protection des consommateurs**. Ce droit vise à garantir au consommateur le pouvoir de disposer des données qu'il a fournies à un prestataire de services afin qu'elles puissent être utilisées ailleurs. Il a été introduit dans le RGPD à cause de *Facebook*, afin de forcer le géant du web à remettre à ses utilisateurs, à leur demande, les données qu'ils ont stockées sur les *posts*, les photos, les *followers*, les amis et les *likes*, afin qu'ils puissent plus facilement changer pour la concurrence. L'idée, qui partait d'un bon sentiment, était que cela obligerait Facebook à adopter des déclarations de protection des données moins unilatérales, car sinon il serait plus facile pour les utilisateurs de se tourner vers la concurrence. Tout cela semble un peu naïf : en pratique, cela n'a eu aucun effet dans ce sens[117]. Mais ce droit existe. Il ne s'applique pas seulement à Facebook mais à tout le monde et doit être respecté.

[131] D'un point de vue juridique, cette nouvelle règle s'applique lorsqu'un responsable du traitement traite des données de manière automatisée en vue de conclure ou d'exécuter un contrat avec la personne concernée, ou sur la base de son consentement. Quelles que soient les données personnelles que le responsable du traitement reçoit de la personne concernée (en sa qualité de responsable du traitement et non de sous-traitant), il doit à tout moment, sur demande, les remettre gratuitement à la personne concernée, dans **un format électronique couramment utilisé**. Compte tenu de l'objectif de cette norme, cela signifie un format qui permette la lecture automatique des données dans un système informatique sous une forme structurée. Un fichier « csv » ou XML serait donc admissible, mais pas un fichier PDF (sauf si les données elles-mêmes sont déjà au format PDF). La personne concernée peut même demander que les données ne lui soient pas envoyées à elle mais directement transmises à un autre responsable du traitement – par exemple un fournisseur de service concurrent. Il faut encore pour cela que le concurrent puisse recevoir ces données. Il ne s'agit toutefois pas d'une obligation du concurrent. Il n'y a qu'une obligation de remettre les données, pas de les accepter. Une exception pourrait être prévue lorsque l'effort nécessaire à la remise ou à la transmission des données serait disproportionné (pour celui qui les fournit). Le Conseil fédéral doit encore préciser cette exception dans l'ordonnance. Cependant, les coûts engendrés par le développement d'une fonction d'exportation de données dans le

115 FF 2017 6685.

116 Art. 20 RGPD.

117 La raison souvent la plus importante pour laquelle les utilisateurs de médias sociaux restent sur une plateforme – leurs *followers* et leurs *likes* – ne peut leur être enlevée, même avec un droit à la remise des données, qu'elle qu'en soit la portée.

logiciel du responsable du traitement ne devraient en principe pas être pertinents à cet égard, puisque la remise et la transmission de données est une obligation légale – et que le responsable du traitement doit concevoir ses systèmes dès le départ de manière à pouvoir s'y conformer (art. 7 al. 1 et 2 nLPD).

[132] Les **exceptions** à l'obligation de transmission sont les mêmes que pour le droit d'accès, par renvoi de l'art. 29 al. 1 nLPD, même si le droit à la remise et à la transmission des données est – par nature – un droit distinct. Il suffit d'examiner leur pertinence respective : contrairement au droit d'accès, le droit à la transmission des données permet en pratique seulement au client du responsable du traitement d'exiger la restitution des données et, en outre, uniquement celles qu'il a lui-même fournies. L'invocation du secret professionnel ou d'autres obligations légales ne devrait guère poser de problème. De même, l'intérêt prépondérant de tiers ne devrait pas être invoqué souvent : même si les données à communiquer contiennent également des données personnelles de tiers – le cas typique de cette exception – l'intérêt de ces derniers n'est pas susceptible de l'emporter sur celui de la personne concernée, puisque, par définition, les données concernées sont celles que le responsable du traitement a reçues du client lui-même, c'est-à-dire des données que le client connaît déjà. Les intérêts prépondérants du responsable du traitement lui-même devraient principalement résider dans les investissements liés à la remise des données. Toutefois, il faut s'attendre à ce que la jurisprudence considère cela comme non pertinent, à l'exception de certains cas exceptionnels, au motif que la question du coût de la remise a déjà été réglée par le législateur. Il est également peu probable que l'intérêt de préserver des secrets d'affaires soit invoqué, car l'obligation de remise des données vise à favoriser la concurrence. En outre, l'argument de l'intérêt prépondérant ne s'applique que si le responsable du traitement ne communique pas les données à un tiers, ce qui sera pourtant souvent le cas (et le responsable du traitement sera donc d'emblée empêché de se prévaloir de son intérêt prépondérant).

[133] Enfin, il reste l'exception de l'utilisation **manifestement abusive ou procédurière.** Bien que ce dernier cas soit probablement tout à fait concevable, la notion d'abus manifeste pose problème étant donné que la remise des données elle-même poursuit un objectif qui est étranger à la protection des données. L'exception doit donc être comprise de manière à ce que la remise de données puisse être refusée si elle vise manifestement en premier lieu un objectif autre que celui prévu par la loi (N 125). Comme pour le droit d'accès, la raison pour laquelle la remise des données est refusée, restreinte ou différée doit justement être en lien avec ce droit à la remise des données.

[134] L'importance de ce nouveau droit des personnes concernées est donc tout sauf évidente, même deux ans après l'entrée en vigueur du RGPD. Il est fort probable que le droit à la portabilité des données n'aura pas une grande importance en pratique en raison de ses restrictions. Tout d'abord, seules les données que la personne concernée a « communiquées » au responsable du traitement peuvent être réclamées. Cependant, selon la définition légale[118], cela couvre non seulement les données qui ont été communiquées mais également les données qui ont été rendues accessibles. Ce qui provient en revanche de tiers n'est pas couvert. En outre, seules des données *personnelles* peuvent être demandées, et uniquement les nôtres. Pour un exemple d'application classique en dehors de Facebook, prenez un service de streaming de musique, sur lequel les utilisateurs peuvent créer leurs listes de lecture. Ils ont la possibilité de demander que les listes de lecture et les informations – comme les noms des artistes qu'ils suivent – soient transférées.

118 Art. 5 let. e nLPD.

Il en va de même du patient qui demande à un hôpital de lui communiquer les données médicales collectées par lui ou sur lui sous forme électronique, afin de les faire analyser ailleurs ou de les mettre à disposition de la recherche. Les données non fournies par le patient lui-même sont considérées comme « communiquées » si celui-ci s'est mis à disposition pour les mesures ou observations correspondantes, et doivent également être remises.

[135] Qu'en est-il toutefois des emails qu'un employé a stockés sur le serveur de son employeur dans le cadre de son activité professionnelle ? Peut-il les emporter avec lui après son licenciement parce qu'il veut les utiliser chez son nouvel employeur ou dans sa propre entreprise ? La remise des données n'est pas techniquement difficile, il s'agit de ses données personnelles et, comme elles sont systématiquement communiquées à des tiers, l'ancien employeur ne peut invoquer ses intérêts prépondérants (tels que la protection de ses secrets d'affaires). Au mieux, on pourrait faire valoir qu'une demande de remise des données serait contraire au but prévu parce qu'il ne s'agit pas d'un consommateur, mais la validité de cet argument semble incertaine[119]. De même, l'invocation d'intérêts prépondérants de tiers ne paraît pas pertinente : l'employé en question ne se verrait pas accorder ce qu'il n'avait pas déjà avant son départ. Il reste tenu de respecter la protection des données même après son départ, pour autant qu'il vive dans un pays où la protection des données est adéquate. Enfin, on pourrait faire valoir qu'il demande plus que ses données personnelles au sens strict, à savoir l'ensemble du contenu de ses emails. Cependant, dans le cadre de l'art. 28 nLPD, la limitation aux données personnelles « en tant que telles », comme dans le cas du droit d'accès, ne s'applique pas, et si le contenu de l'obligation de remise des e-mails devait être interprété de manière aussi restrictive, l'obligation de remettre le contenu d'une playlist semblerait également discutable. Certes, ces « conséquences non voulues » prévisibles ne semblent pas avoir dissuadé le Parlement suisse, pas plus que celui de l'UE ; en Suisse, l'introduction de la portabilité des données a été le résultat d'une concession politique en faveur de la gauche, qui souhaitait un renforcement considérable de la LPD.

[136] Au demeurant, la violation du droit à la remise des données n'est pas **punissable pénalement** (pas même la transmission intentionnelle de données incomplètes ou incorrectes). Comme elle ne vise pas à protéger la personnalité, une telle violation ne rend pas non plus illicite le traitement de données auquel elle se rapporte. Elle ne peut être mise en œuvre que par une action civile ou par le PFPDT au moyen d'une ordonnance.

D. Droit de rectification et « droit à l'oubli »

[137] Le droit de rectification qui figurait auparavant à l'art. 5 al. 2 LPD a été déplacé à l'art. 32 nLPD, qui prévoit également la possibilité d'agir en justice pour faire valoir ses droits. En revanche, le droit d'opposition se trouve, comme auparavant, à l'art. 30 al. 2 let. b nLPD (et à l'art. 30 al. 3 nLPD ; cf. également N 38).

[138] Le **droit d'opposition** existait déjà par le passé et n'a pas été modifié dans la révision de la LPD. Ainsi, en dépit des lamentations[120], la Suisse a toujours eu un « droit à l'oubli ». Il ne

119 Le caractère inapproprié serait probablement plus évident si l'employé d'une entreprise voulait obtenir les données relatives à toutes ses entrées et sorties enregistrées sur son badge. Il n'est pas évident de voir comment il pourrait continuer à utiliser ces données pour la finalité initiale ou comment il pourrait atteindre la finalité de la norme d'une autre manière grâce à cette remise des données.

120 Cf. par exemple le postulat CN 12.3152 de Jean Christophe Schwaab.

s'applique pas de manière absolue, dès lors qu'il est limité dans le secteur privé par les motifs justificatifs prévus à l'art. 31 nLPD. Contrairement au RGPD, qui distingue entre de très complexes droits d'opposition, de limitation et de suppression[121], le concept suisse est tout simple : la personne concernée peut non seulement s'opposer au traitement de ses données personnelles dans son ensemble (c'est-à-dire demander l'interruption du traitement ou la suppression de ses données), mais également à des aspects ou à des formes particulières de traitement. Cela lui donne beaucoup plus de liberté et permet de mieux prendre en compte les particularités du cas concret, car en cas de litige les effets de l'opposition peuvent être limités aux aspects du traitement des données qui ne sont pas justifiés en vertu de l'art. 31 nLPD. Si, par exemple, une personne demande la suppression de toutes ses données pour toutes les finalités du traitement, le responsable du traitement peut se borner à ne supprimer les données que pour certaines finalités s'il a de bonnes raisons (comme une obligation légale) de les traiter à d'autres fins.

[139] Dans le cadre du **droit de rectification**, il peut être exigé que des données incorrectes soient supprimées ou corrigées. Il s'agit d'une règlementation complexe, il est donc surprenant qu'elle n'ait pas vraiment été discutée au Parlement. En effet, contrairement au droit d'opposition, le droit de rectification est beaucoup plus absolu dans sa formulation. Si un responsable du traitement veut se défendre contre une demande de rectification, il ne peut faire valoir que les deux motifs énumérés à l'art. 32 al. 1 nLPD, à savoir que la loi interdit toute modification (p. ex. en cas d'obligation de conservation) ou que les données personnelles sont traitées à des fins d'archivage dans l'intérêt public (ce qui se produira rarement dans le secteur privé). Les motifs justificatifs énumérés à l'art. 31 nLPD ne s'appliquent pas[122], c'est-à-dire que le responsable du traitement ne peut pas prétendre, par exemple, que la modification est beaucoup trop coûteuse ou qu'il existe un intérêt supérieur à laisser telles quelles les données incorrectes. Ce dernier point peut sembler absurde à première vue, mais il faut garder à l'esprit qu'une violation du principe de l'exactitude des données selon l'art. 6 al. 5 nLPD peut être justifiée par l'art. 31 nLPD. En d'autres termes, le législateur prévoit qu'un responsable du traitement peut continuer à traiter des données incorrectes s'il a de bonnes raisons de le faire, alors que ce même législateur l'oblige à corriger ces données si la personne concernée le demande. Prenons le cas où un client d'une société demande que son nom mal orthographié soit corrigé non seulement dans le fichier client (ce que la société fera certainement), mais aussi dans toutes les copies de sauvegarde que cette même société conserve (ce que la société n'est pas tenue de faire en vertu de l'art. 6 al. 5 nLPD en relation avec l'art. 31 nLPD, car l'effort est disproportionné par rapport au bénéfice, ce qui confère un intérêt prépondérant au responsable du traitement). Selon le libellé de l'art. 32 al. 1 nLPD, la personne concernée devrait néanmoins pouvoir contraindre la société à le faire. Le message du Conseil fédéral indique même que le droit de rectification devrait également exister même en l'absence d'atteinte à la personnalité, c'est-à-dire sans violation de la protection des données[123]. On peut douter que cette affirmation ait été réfléchie jusqu'au bout – et que sa conséquence ait été réellement voulue.

[140] Dans la pratique, cette conception erronée et cette contradiction dans la nLPD devront être rectifiées de deux manières : *premièrement*, le responsable du traitement devra pouvoir invoquer un **abus de droit** si l'exercice du droit de rectification constitue un procédé dilatoire ou s'il va si

121 Art. 17, 18, 21 et 22 RGPD.

122 FF 2017 6693.

123 FF 2017 6693.

loin qu'il ne sert plus réellement à protéger la personnalité (art. 1 nLPD) et qu'il est donc contraire à l'objectif poursuivi. *Deuxièmement*, la question de l'exactitude des données – contrairement à ce que le message du Conseil fédéral laisse entendre – devra être appréciée selon le principe de l'art. 6 al. 5 nLPD. Cela correspond également à ce que prévoit l'art. 16 RGPD. Selon l'art. 32 al. 1 nLPD, les données ne sont donc considérées comme incorrectes qu'au regard de la **finalité de leur traitement**. Le but de l'archivage des données est de sauvegarder l'état des données telles qu'elles étaient avant. Par conséquent, aucune correction ne peut être exigée tant qu'il est garanti que – en cas de restauration des données – les modifications apportées entre-temps dans le système opérationnel sont mises à jour.

[141] La révision n'a pas modifié la possibilité de demander un ***disclaimer*** tant qu'il n'est pas clair si les données sont incorrectes (une particularité suisse) et le droit à ce qu'une correction, un *disclaimer*, une suppression ou une interdiction de traitement soit communiqué à des tiers. Toutefois, la communication à des tiers ne peut être demandée que dans le cadre d'un procès. A cet égard, la Suisse va moins loin que l'art. 19 RGPD, selon lequel les rectifications de données personnelles et les limitations du traitement doivent également être notifiées sur demande aux **destinataires auxquelles les données ont été communiquées**. En Suisse, cela ne s'applique pas sous cette forme.

IV. Mesures d'accompagnement

A. Registre des activités de traitement

[142] À l'avenir, conformément à l'art. 12 nLPD, toute personne privée responsable du traitement et tout sous-traitant devra tenir un **registre de ses activités de traitement**, c'est-à-dire que pour chaque activité de traitement, les informations requises par la loi devront être enregistrées. Cette règle a été reprise du RGPD[124]. Les registres créés pour le RGPD peuvent par conséquent être repris ; les seules informations qui doivent être ajoutées à cet égard sont celles relatives aux pays tiers (ou régions ; cf. N 95) vers lesquels les données personnelles sont exportées (y compris les pays de l'EEE[125]) ainsi que les garanties sur lesquelles le responsable du traitement se fonde lorsqu'il s'agit de transfert de données vers des pays tiers peu sûrs[126]. La nLPD ne prévoit toutefois pas d'obligation générale de documentation comparable à l'art. 5 al. 2 RGPD ; cette obligation était encore envisagée dans l'avant-projet, mais a par la suite été abandonnée. Une telle obligation peut néanmoins découler des art. 7 ss nLPD. L'**exception pour les PME** prévue à l'art. 12 al. 5 nLPD ne jouera probablement pas de rôle dans la pratique en raison de ses conditions restrictives.

[143] Toutefois, l'obligation d'enregistrer les collectes de données prévue à l'art. 11a LPD a été supprimée ; dans la pratique, elle avait de toute façon été largement ignorée. Par conséquent, la nLPD ne contient plus de disposition qui oblige les responsables du traitement à s'enregistrer ou à enregistrer leurs opérations de traitement. Les personnes privées responsables du traitement ne sont donc soumises qu'aux obligations d'annonces en cas de communications à l'étranger (N 65 ss), des conseillers à la protection des données (N 168 ss), des représentants des respon-

124 Art. 30 RGPD.

125 Du point de vue du RGPD, en revanche, les transferts de données vers d'autres pays de l'EEE ne constituent pas des transferts vers des pays tiers.

126 Art. 12 al. 2 let. g nLPD.

sables du traitement étrangers (N 172 ss), des violations de la sécurité des données (N 160 ss), ainsi qu'à l'obligation de consulter le PFPDT dans le cas de projets à haut risque après une évaluation de l'impact sur la protection des données (N 148 ss).

[144] Il n'existe pas de règle fixe quant à la manière de répartir l'ensemble des traitements de données d'une entreprise selon les buts du registre. Il s'est avéré judicieux de regrouper les **opérations de traitement ayant un lien entre elles**, à condition qu'elles aient les mêmes paramètres essentiels de protection des données. Le registre n'est pas une fin en soi, mais il devrait aider au respect de la protection des données et à fournir au responsable du traitement et au sous-traitant une vue d'ensemble des activités de leur entreprise en rapport avec la protection des données. Si le PFPDT enquête sur une affaire, la première chose qu'il fera sera de demander ce registre. L'expérience du RGPD démontre que de nombreux registres ont tendance à être trop détaillés. A titre d'exemples d'activités d'un responsable du traitement figurent : l'administration du personnel, le recrutement, la gestion des données relatives aux clients, le service client, la boutique en ligne, la newsletter, le développement de produits, la gestion des fournisseurs, les finances et la comptabilité, le site Internet, la vidéosurveillance, la gestion des installations, les emails, les affaires contentieuses et les enquêtes internes.

[145] Il n'existe aucune **exigence formelle** ; un document Excel ou Word est tout aussi acceptable qu'une solution informatique sophistiquée, telle que le proposent certaines entreprises. Le registre peut être géré de manière décentralisée, et sa gestion peut elle-même être déléguée (p. ex. à un responsable conjoint du traitement ou à un prestataire de services). Cependant, le registre doit contenir *toutes* les activités de traitement et être à jour. La violation de l'obligation de tenir un registre n'entraîne pas de sanction directe. Le PFPDT peut demander à consulter le registre, mais pas les personnes concernées. Elles peuvent toutefois obtenir des informations équivalentes grâce au droit d'accès. Les déclarations de protection des données contiennent aussi souvent des informations similaires à celles contenues dans les registres de traitement ; elles sont aussi souvent élaborées ensemble.

[146] Le registre contient les **données clés en termes de protection des données** des différentes activités de traitement de données, mais il ne contient pas de données personnelles et il ne s'agit pas d'un journal des traitements de données. L'art. 12 al. 2 et 3 nLPD énumère les éléments qui doivent nécessairement figurer dans le registre. L'identité du responsable du traitement ne fait pas référence aux personnes responsables à l'interne, mais généralement à la personne morale. S'il y a plusieurs personnes responsables, toutes doivent être répertoriées. Par finalité du traitement, on entend la finalité à laquelle sert l'activité de traitement (p. ex. l'enregistrement des heures de travail, la comptabilisation des salaires, le service à la clientèle, les achats, la gestion des voyages, etc.). Les utilisations ultérieures (p. ex. *via* un *data warehouse*) sont généralement des activités de traitement distinctes. Lors de la description des catégories de données personnelles, il est possible de résumer (p. ex. les données de contact, les données bancaires, les évaluations, la correspondance, les emails, les documents relatifs à un projet, les heures de travail, les données contractuelles). Il en va de même pour les personnes concernées (p. ex. les clients, les employés) et les destinataires (p. ex. les sociétés du groupe, les prestataires de services, les autorités, les médias, le public). Les responsables conjoints du traitement sont également des destinataires. La durée de conservation doit être indiquée directement (p. ex. tant qu'un compte client existe, dix ans après la fin du contrat) ou à l'aide des critères qui la déterminent (p. ex. les durées de conservation en vertu du droit commercial, l'intérêt à fournir des preuves, la conservation légale). En ce qui concerne la sécurité des données, il est conseillé de se référer aux lignes directrices per-

tinentes en matière de sécurité informatique et, si nécessaire, de mentionner ce qui va au-delà de la protection de base. En cas de transferts de données depuis la Suisse, il convient d'indiquer les pays destinataires, des termes génériques bien définis tels que « Europe » ou « monde » étant suffisants. Les « clauses contractuelles types de l'UE » ou les « *Binding Corporate Rules* » sont des exemples de garanties à mentionner en cas de transferts de données vers des pays tiers peu sûrs, si tant est qu'il y en ait.

[147] Les **sous-traitants** doivent également tenir un registre, comprenant entre autres les noms de leurs clients (cela peut se faire par référence à la base de données clients et il n'est pas nécessaire d'y inscrire les responsables conjoints du traitement). En ce qui concerne les catégories de traitement, des descriptions génériques (p. ex. services d'exploitation informatique, enregistrement des visiteurs du site et fonctionnement d'une ligne de vente par correspondance) sont suffisantes.

B. Analyse d'impact relative à la protection des données

[148] L'analyse d'impact relative à la protection des données – ou « AIPD » – a connu une popularité croissante en tant qu'outil de *compliance* ces dernières années. Il est désormais l'outil de choix pour valider et justifier les traitements de données plus sensibles du point de vue du respect de la protection des données. Aujourd'hui déjà, si un projet doit être soumis au PFPDT pour évaluation, il arrive régulièrement que le PFPDT requiert une AIPD. Il s'agit essentiellement d'une **auto-évaluation de la protection des données** pour des projets qui semblent un peu plus sensibles de ce point de vue. Cette évaluation est désormais requise dans certains cas par l'art. 22 nLPD.

[149] Lors d'une AIPD, le projet est tout d'abord décrit sous l'angle du traitement des données (quelles données sont traitées, par qui, dans quel but, comment et où, et, le cas échéant, quelles données sont transmises). Ensuite, le « risque pour la personnalité » de la personne concernée est analysé et décrit. Le message du Conseil fédéral reste vague et abstrait à cet égard[127]. En pratique, cependant, ce ne sont pas les violations des droits de la personnalité en tant que telles qui sont régulièrement évaluées, mais plutôt les **conséquences négatives** que le traitement des données pourrait avoir avec une certaine vraisemblance pour la personne concernée. Le traitement des données peut avoir des conséquences physiques (des données erronées peuvent conduire à un mauvais traitement médical, la divulgation de données relatives aux opinions politiques d'une personne peut conduire à ce que celle-ci soit harcelée ou menacée, la perte de confidentialité peut causer de l'anxiété, etc.) ou des conséquences matérielles (une personne se voit refuser un emploi, sa carte de crédit est utilisée de manière frauduleuse, elle est victime de chantage, des moyens de preuve sont falsifiés ou perdus, elle subit des frais injustifiés, elle doit fournir un effort supplémentaire pour corriger des erreurs, etc.) ou encore des conséquences immatérielles (inconvénients d'ordre social, l'« expérience troublante » que représente une atteinte à la vie privée ou une intimidation telle que les personnes concernées cessent de faire certaines choses, etc.)[128].

127 FF 2017 6677.

128 Pour plus d'examples, cf. : Fraunhofer Institute for Systems and Innovation Research ISI, The Data Protection Impact Assessment According to Article 35 GDPR, A Practicioner's Manual, Fraunhofer Verlag 2020, p. 39 ss (http://publica.fraunhofer.de/documents/N-590015.html (état au 9 mars 2021).

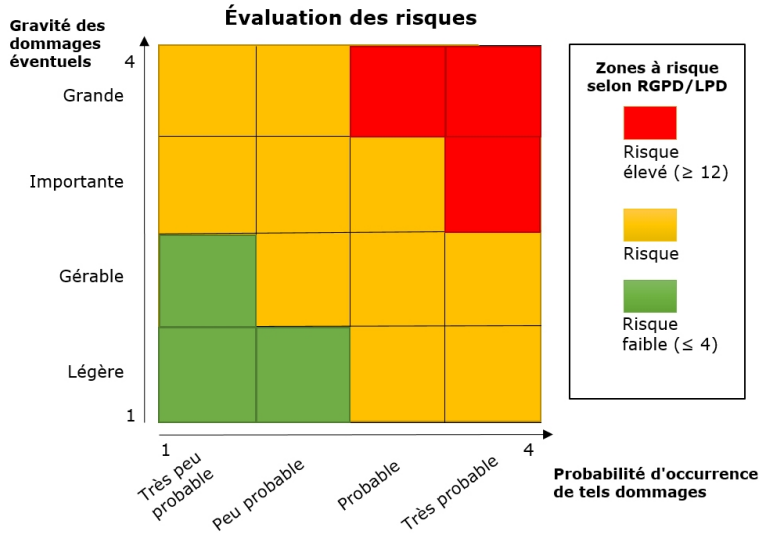
[150] Enfin, l'AIPD indique quelles **mesures** techniques et organisationnelles peuvent **prévenir ces conséquences négatives** ou au moins les limiter, et parmi ces mesures lesquelles sont déjà prises et lesquelles restent à prendre. Nombre de ces mesures seront déjà préconisées dans le cadre de la LPD, telles que la restriction de l'accès aux données sur la base du « besoin de savoir », la limitation de la période de conservation, la garantie de la sécurité des données, la pseudonymisation en amont, la vérification de l'exactitude des données, le principe des « quatre yeux » pour les décisions importantes, des règles claires sur le traitement des données, ainsi que la formation et la supervision du personnel.

[151] Dans un cas simple (p. ex. lors de la mise en place d'une caméra de surveillance), une AIPD peut être très courte et schématique, alors que dans des projets plus importants, elle peut devenir très complexe. En outre, il n'est pas nécessaire de l'effectuer séparément pour chaque traitement de données ; une AIPD peut être effectuée pour plusieurs projets présentant les mêmes risques (p. ex. une AIPD pour toutes les caméras de sécurité, dans laquelle il est enregistré où et comment les caméras doivent être installées). Bien que la **« justification » du traitement des données** ne fasse pas formellement partie du contenu minimum d'une AIPD, elle sera néanmoins souvent nécessaire car il s'agit de prendre uniquement en compte les conséquences négatives involontaires ou même *injustifiées*. Prenons l'exemple de la caméra de surveillance : pour le vandale qui est arrêté à l'aide de ces enregistrements, cela a une conséquence négative, sans pour autant représenter un risque élevé. En revanche, si elle est utilisée pour surveiller en permanence le comportement au travail d'employés pourtant irréprochables, elle pose alors problème. A l'inverse, un risque élevé ne nécessite pas une atteinte concrète à la personnalité avec des conséquences graves. Une probabilité assez élevée qu'elle se produise suffit. La question de savoir si le risque élevé conduit à l'inadmissibilité du traitement des données est quant à elle évaluée, dans le secteur privé, à l'aune des art. 6, 7, 16, 17, 30 et 31 nLPD.

[152] Une AIPD doit en principe être **réalisée par le responsable du traitement lui-même**. Il ne s'agit ni d'un audit ni d'une évaluation par un tiers de la conformité à la protection des données. L'expert interne ou externe en matière de protection des données peut cependant l'assister : si le contenu d'une AIPD doit provenir de la personne responsable dans l'entreprise, car c'est elle qui connaît le mieux les faits, l'expert veille à ce que les bonnes questions soient posées et à ce que les conclusions soient formulées de manière appropriée (c'est-à-dire du point de vue de la protection des données). Une AIPD inclut généralement un examen de la conformité avec la LPD (ou le RGPD, qui connaît également l'AIPD[129]).

[153] Une AIPD répond dès lors à la question de savoir si le projet, malgré toutes les mesures qui ont été ou doivent être mises en œuvre, comporte un **« risque élevé »** pour la personnalité des personnes concernées. Le risque est la combinaison de sa probabilité d'occurrence et de la gravité du dommage (cf. graphique). Lorsqu'il y a une probabilité assez élevée que des conséquences indésirables assez graves se produisent, il faut considérer que le risque est élevé.

129 Art. 35 RGPD.



[154] L'expérience montre qu'après avoir effectué une AIPD, très peu d'entreprises concluront que, malgré toutes les mesures prises, il existe un risque élevé. Il est fréquent qu'un projet soit conçu de telle manière que l'AIPD arrive à la conclusion qu'il n'y a *pas* (ou plus) de risque élevé et que le responsable du traitement décide donc de mettre en œuvre ou de poursuivre le projet. Concernant l'entrée en vigueur de la nLPD, il n'existe aucune règle selon laquelle tous les traitements de données potentiellement sensibles devraient être examinés au moment de l'entrée en vigueur de la nouvelle loi. Toutefois, en règle générale, une AIPD doit être réalisée environ tous les trois ans[130] ou lorsque le traitement des données est modifié sur des points essentiels ou encore lorsque les circonstances ont changé de manière significative.

[155] Si, contre toute attente, un risque élevé ne peut être écarté, le projet doit être **soumis au PFPDT pour consultation**, qui l'évaluera dans un délai de deux à trois mois et proposera, le cas échéant, de nouvelles mesures ou l'arrêt du projet (art. 23 nLPD). Cette obligation de consultation est l'une des raisons pour lesquelles les entreprises feront tout leur possible pour éviter cette étape. Si le « risque élevé » ne peut être évité, il est donc plus probable qu'elles désignent un « conseiller à la protection des données » au sens de l'art. 10 nLPD (N 168 ss), qui évaluera le projet à la place du PFPDT (art. 23 al. 4 nLPD). Des délais beaucoup plus courts peuvent être convenus avec le conseiller à la protection des données et celui-ci peut également s'avérer moins critique. Une autre possibilité d'éviter l'AIPD est la certification au sens de l'art. 13 nLPD (qui n'aura toutefois que peu d'intérêt en pratique, au vu des expériences passées en matière de certification), ou l'utilisation d'un code de conduite évalué par le PFPDT (N 175 ss), qui pourrait être intéressante pour certaines branches.

[156] Cela soulève la question de savoir **quand une AIPD est obligatoire**. Ici, le texte de l'art. 22 al. 1 et 2 nLPD n'est à première vue pas clair, ce qui est dû à une erreur dogmatique[131]. Une

130 Recommandation du Groupe de travail « Article 29 » sur la protection des données, Lignes directrices concernant l'analyse d'impact relative à la protection des données (AIPD) et la manière de déterminer si le traitement est « susceptible d'engendrer un risque élevé » aux fins du règlement (UE) 2016/679 (WP 248), état au 4 avril 2017, p. 12 (dans la dernière version du 4 octobre 2017, cette référence a toutefois été supprimée) (https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236 (état au 9 mars 2021)).

131 La disposition part du principe qu'avant une AIPD les traitements de données ne disposent pas encore de mesures de protection des personnes concernées et que l'AIPD détermine les mesures à prendre. Par conséquent, il existe un

AIPD est obligatoire si un traitement de données peut, de par sa nature, comporter un risque élevé pour la personne concernée[132]. Seuls les résultats de l'AIPD montreront si le projet, quelles que soient les mesures prises ou à prendre, comporte effectivement un risque élevé. En ce sens, l'al. 2 n'énumère que deux cas dans lesquels un tel *soupçon* existe (au sens d'une fiction) et où une AIPD est donc obligatoire. Toutefois, contrairement à son libellé, l'al. 2 ne dit *pas* que ces deux cas – un traitement étendu de données personnelles particulièrement sensibles ou une surveillance systématique de grandes parties du domaine public – comportent en eux-mêmes un risque particulièrement élevé. Considérons une base de données contenant de nombreuses déclarations publiques d'hommes politiques (données sur les « opinions politiques ») : bien qu'elle requiert une AIPD, elle ne comporte en principe pas pour autant de risque élevé.

[157] Si aucun des deux cas prévus à l'al. 2 ne s'applique, il convient d'évaluer, sur la base de la manière dont les données sont traitées, si elles peuvent entraîner un risque élevé pour les personnes concernées en cas de non-respect des restrictions et des mesures supplémentaires à prendre (ce qui détermine le « risque brut », tandis que le « risque net » résultera de l'AIPD). En d'autres termes, une AIPD est nécessaire lorsque le traitement des données est en lui-même ***sensible*** du point de vue de la protection des données. Le Groupe de travail « Article 29 » de l'UE a élaboré pour le droit communautaire, qui dispose d'une règle comparable avec l'art. 35 RGPD, un catalogue des facteurs de risque[133]. Si deux des **facteurs de risque** sont présents, en règle générale, une AIPD doit être effectuée. Ces facteurs de risque comprennent : la surveillance systématique, le traitement de données confidentielles ou hautement personnelles, l'évaluation des aspects personnels d'une personne, le traitement étendu de données, la comparaison ou mise en relation de différentes sources de données, l'utilisation innovante de la technologie, l'entrave à l'utilisation d'un service ou à la conclusion d'un contrat, le traitement de données de personnes vulnérables et les décisions individuelles automatisées. Dans l'UE, les autorités de protection des données publient d'autres listes noires et blanches de cas dans lesquels une AIPD doit ou ne doit pas être exécutée. En Suisse, le PFPDT pourra également le faire ou l'ordonnance pourra le prévoir.

[158] Lors des débats parlementaires, le **profilage** a été supprimé de l'art. 22 al. 2 nLPD, car il existe de nombreux profilages qui ne sont pas sensibles. Mais qu'en est-il du profilage « à risque élevé » ? Il faut ici opérer une distinction : si le profilage conduit à un profil de la personnalité (N 24 ss), une AIPD devra généralement être effectuée. Toutefois, si cette dernière arrive à la conclusion qu'il n'y a pas de risque élevé, compte tenu des mesures prises, deux possibilités existent : soit l'on suppose qu'il ne s'agit pas d'un profilage « à risque élevé ». Selon une interprétation littérale et systématique de la définition de l'art. 5 let. g nLPD, un tel risque n'est présent que si le fait que le profilage entraîne un profil de la personnalité comporte en lui-même un risque élevé pour la personne concernée (N 27 ss). Un profil de la personnalité généré par ordinateur

risque *avant* et un risque *après* l'AIPD. La réalité est cependant différente : aujourd'hui, le traitement des données – conformément à l'art. 7 nLPD – est souvent conçu dès le départ de manière à ce que les risques soient suffisamment faibles. Dans ce cas, une AIPD confirme simplement que le risque n'est pas élevé. Elle doit néanmoins être effectuée.

132 Il s'agit en réalité d'une double probabilité : une AIPD est nécessaire s'il est probable qu'il soit probable que le traitement des données ait des conséquences graves pour la personne concernée (cf. FF 2017 6676, n. 150).

133 Recommandation du Groupe de travail « Article 29 » sur la protection des données, Lignes directrices concernant l'analyse d'impact relative à la protection des données (AIPD) et la manière de déterminer si le traitement est « susceptible d'engendrer un risque élevé » aux fins du règlement (UE) 2016/679 (WP248 rév. 01), état au 4 octobre 2017, p. 9 ss (https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236 (état au 9 mars 2021)).

n'est alors pas suffisant à lui seul. Par conséquent les entreprises prendront les mesures appropriées afin d'éviter que le profilage « à risque élevé » ne se produise dans la pratique, car dans le cas contraire il faudrait consulter le PFPDT ou nommer à la place un conseiller à la protection des données. Soit, alternativement, l'on peut estimer que, même si le profilage « à risque élevé » existe à partir du moment où il conduit à un profil de la personnalité, il ne constitue qu'une partie d'un traitement de données dans lequel ce risque est minimisé sur une base nette grâce aux mesures prises et, par conséquent, aucune consultation du PFPDT n'est nécessaire.

[159] Dans la nLPD, contrairement au RGPD, la violation de l'obligation d'effectuer une AIPD n'est **pas sanctionnée par une amende**. Elle ne peut pas non plus être poursuivie en justice par les personnes concernées. Seul le PFPDT peut ordonner sa mise en œuvre.

C. Obligation d'annoncer les violations de la sécurité des données

[160] La nLPD introduit pour la première fois en Suisse l'obligation de procéder à des *Data Breach Notifications* : à l'avenir, en cas de perte de données, d'email envoyé par erreur ou de tout autre incident lié à la sécurité des données, il sera nécessaire d'en **informer le PFPDT**. Le RGPD prévoit déjà une telle obligation de notification[134] et elle a déjà donné lieu à de nombreuses notifications[135]. La Suisse a opté pour une réglementation un peu plus légère, qui obligera néanmoins toutes les entreprises à définir les responsabilités et prévoir des processus appropriés.

[161] Selon l'art. 5 let. h nLPD, il y a **violation de la sécurité des données** lorsque la confidentialité, l'intégrité ou la disponibilité de données personnelles[136] est affectée de manière imprévue au cours du traitement des données et que cela entraîne la perte de données personnelles, leur modification, leur effacement ou leur destruction, leur divulgation ou encore un accès non autorisés à ces données. Cela peut être causé par une cyberattaque ou par des autorités étrangères qui accèdent aux données stockées dans le cloud, ainsi que par une mauvaise manipulation à l'interne, qui conduit à la divulgation de données confidentielles au mauvais client, à la perte de données personnelles en raison d'un *ransomware* ou d'une erreur de système, ou à un employé qui fait son « propre truc » avec des données personnelles externes en violation de ses instructions. Toutefois, lorsque le responsable du traitement va simplement trop loin dans ses projets concernant les données personnelles, par exemple en les détournant à d'autres fins ou en les stockant pendant une durée disproportionnée, cela peut constituer une violation de la protection des données, mais il ne s'agit pas pour autant d'une violation de la sécurité des données. Cette notion correspond à celle du RGPD[137] .

[162] Ces violations de la sécurité des données ne doivent être annoncées que s'il existe **un « risque élevé » de conséquences négatives** pour la personne concernée. Bien entendu, une évaluation au cas par cas est nécessaire. Mais en règle générale, la question suivante peut faciliter l'évaluation : Quelle est la probabilité que la violation ait une conséquence négative détermi-

134 Art. 33 et 34 RGPD.

135 DLA Piper GDPR Data Breach Survey 2020, https://www.dlapiper.com/en/uk/insights/publications/2020/01/gdpr-data-breach-survey-2020 (état au 9 mars 2021).

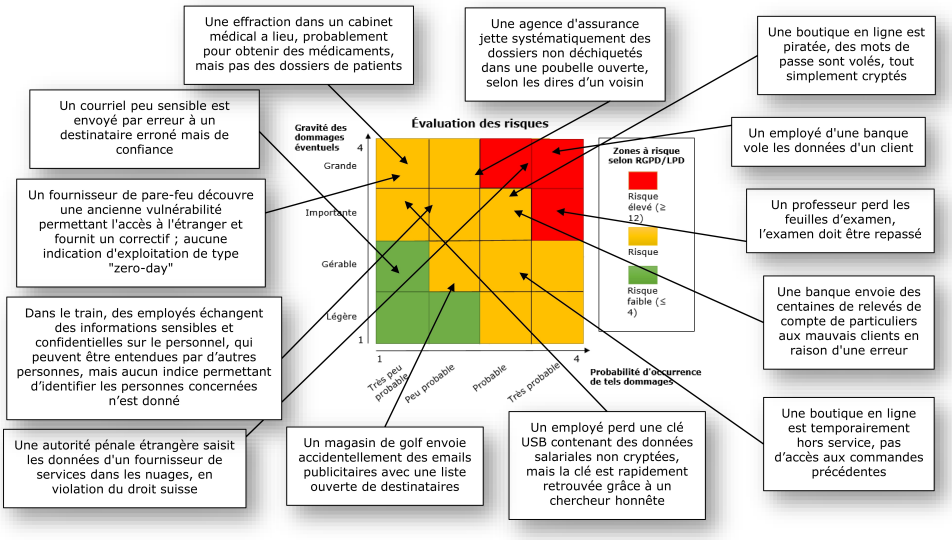
136 Ces trois éléments sont ce que l'on entend généralement par « sécurité ».

137 Art. 4 ch. 12 RGPD.

née[138] sur la personne concernée (faible, moyenne, élevée) et comment cette conséquence négative serait-elle qualifiée (légère, moyenne, grave) ? Si une conséquence négative grave est au moins probable ou si une conséquence négative moyenne est très probable, le risque est élevé[139]. Il n'y a **pas de règle *de minimis***. Même si une seule personne est concernée, une annonce peut être nécessaire. Cependant, l'expérience montre que le risque augmente avec le nombre de victimes potentielles. L'art. 24 nLPD n'exige toutefois pas de spéculer sur ce qui pourrait se produire. Seuls les dangers qui semblent réalistes et concrets sur la base des circonstances spécifiques et de l'expérience générale de la vie sont pris en compte. Si, par exemple, un email confidentiel est envoyé par inadvertance à la mauvaise personne, mais que le destinataire est connu et qu'il est raisonnablement digne de confiance et honnête, on ne peut généralement pas présumer un risque élevé. Il en va de même lorsqu'un ordinateur portable avec un disque dur crypté est volé. En revanche, si l'employé d'une entreprise de taille moyenne perd dans la rue une clé USB contenant les données privées et les salaires de tous les employés en texte clair et ne la retrouve pas, il y a probablement un risque élevé pour la personnalité des personnes concernées et une annonce est nécessaire. Si une entreprise découvre, grâce au signalement d'un employé, que certaines données sensibles concernant les employés étaient accessibles à tous les employés durant une période indéterminée dans un sous-dossier non protégé du département des ressources humaines sur le réseau interne de l'entreprise, il n'y a généralement pas de risque élevé, même s'il n'existe pas de journal d'accès, à condition qu'il n'y ait pas d'indice d'utilisation abusive et – comme c'est généralement le cas – qu'il ne faille pas supposer que les employés recherchent activement de telles fuites de données sur le réseau interne. Si les données étaient accessibles sur Internet, la probabilité de telles recherches est beaucoup plus élevée. Et si un hacker accède intentionnellement aux mots de passe d'une boutique en ligne, il faut également présumer un risque élevé si les mots de passe sont cryptés mais que les plus simples peuvent être craqués avec des outils appropriés. Les hackers essaieront généralement de le faire. Pour d'autres cas (ici à l'aide de l'exemple d'une classification des dommages et des probabilités à quatre niveaux, où, selon la LPD, seuls les cas dans la zone rouge doivent être annoncés, alors que, selon le RGPD, même les cas dans la zone jaune entraînent une obligation d'annonce), voir le schéma ci-dessous :

138 Par exemple une atteinte à la réputation, l'humiliation, une perte d'emploi, des pertes financières, une discrimination ou des dommages corporels.

139 En général, on entend par risque le résultat de la probabilité d'occurrence et du montant des dommages.



[163] Le « risque élevé » de l'art. 24 nLPD se distingue du « risque élevé » d'une AIPD (N 152). En effet, dans le contexte de l'art. 24 nLPD, une violation de la sécurité des données a effectivement eu lieu et ses effets sont mesurés. En revanche, dans le cadre d'une AIPD, il s'agit d'évaluer la probabilité que la sécurité des données soit violée ou que surviennent d'autres événements entraînant de graves conséquences du même ordre pour les personnes concernées. Ainsi, la méthode de calcul du risque (probabilité d'occurrence x montant du dommage) est fondamentalement la même (partant, la grille d'évaluation ci-dessus peut également être utilisée aux fins de l'art. 24 nLPD), mais la relation est différente. Le seuil pour admettre un risque élevé est *plus bas* pour l'AIPD.

[164] S'il existe une obligation d'annonce, il faut **avertir le PFPDT le plus rapidement possible.** Il n'y a pas de délai de 72 heures, contrairement au RGPD. L'annonce doit être faite dès que les informations minimales requises par la loi sont réunies : Que s'est-il passé ? Quelles sont les personnes et les données concernées ? Et quelles sont les conséquences possibles ? Quelles mesures ont été prises ou sont prévues pour rétablir la sécurité des données et pour prévenir ou atténuer les conséquences pour les personnes concernées ? Le responsable du traitement ne doit pas entrer dans tous les détails ; si le rapport n'est pas complet parce que les enquêtes sont toujours en cours, cela ne pose pas de problème. Il s'agit seulement pour le PFPDT de pouvoir évaluer si le responsable du traitement maîtrise la situation au mieux et prend les mesures nécessaires. Si ce n'est pas le cas, le PFPDT devra intervenir ; si le premier rapport n'est pas suffisant, il peut et va assurer un suivi. Il sera particulièrement important d'annoncer au PFPDT s'il est prévu d'informer les personnes concernées. Si le responsable du traitement découvre par la suite un nouveau risque élevé, il devra également le signaler. Aucune annonce n'est nécessaire si les personnes concernées ont fait part de leur désintérêt pour une telle annonce. Il n'y a donc plus de risque élevé. La responsabilité principale de la gestion adéquate de la violation incombe au responsable du traitement. Contrairement au RGPD, il n'est cependant pas tenu, en vertu du droit suisse, de tenir une liste des violations de la sécurité des données qui se sont produites.

[165] L'obligation d'annonce décrite ci-dessus incombe uniquement au responsable du traitement. Toutefois, chaque **sous-traitant** a sa propre obligation d'annonce. Cette obligation existe envers le responsable du traitement et va beaucoup plus loin : le sous-traitant doit annoncer le plus rapidement possible toute violation de la sécurité des données dont il a connaissance. Cela s'ap-

plique indépendamment du fait de savoir si la violation présente un risque. Il s'agit dans une certaine mesure d'un inconvénient pour les sous-traitants, tels que les fournisseurs de services informatiques, car ils doivent annoncer à leurs clients toute violation, même insignifiante, de leurs obligations, ce qui peut parfois avoir des conséquences en vertu du droit des contrats, par exemple. Le législateur a voulu laisser au responsable du traitement le soin d'évaluer si une annonce au PFPDT était nécessaire. Il s'agit d'une obligation *légale*, c'est-à-dire que même si elle n'est pas contractuellement convenue, le sous-traitant doit s'y conformer. Elle ne peut pas non plus être restreinte contractuellement. Le respect de la sécurité des données incombe d'ailleurs légalement tout autant au sous-traitant qu'au responsable du traitement.

[166] L'art. 24 nLPD prévoit également d'**informer la personne concernée**, mais cette information ne devrait être requise qu'exceptionnellement[140]. Le critère est de savoir si l'information est « nécessaire pour sa protection ». Il ne s'agit pas de prime abord d'une question de transparence, mais plutôt d'information à fournir lorsque la personne concernée doit *elle-même* prendre des mesures pour se protéger des conséquences de la violation ou pour les atténuer. Il peut s'agir, par exemple, de changer son mot de passe ou de vérifier ses relevés bancaires ou – dans le cas d'une personne célèbre – de se préparer aux questions des journalistes après que des informations privées croustillantes à son sujet aient été volées et communiquées à la presse. En revanche, lorsque le dommage a déjà été causé ou que la personne concernée est déjà informée ou ne peut rien faire d'utile elle-même, il n'y a pas d'obligation d'informer. Cette dernière va également moins loin que l'obligation d'avertir le PFPDT. L'obligation d'informer ne donne pas à la personne concernée un droit de regard sur l'incident et le législateur a prévu diverses exceptions à cette obligation, notamment lorsque cela nécessiterait des efforts disproportionnés pour identifier les personnes à informer ou pour leur fournir ces informations. Contrairement à ce qui est prévu dans le RGPD, une communication publique n'est pas obligatoire dans de tels cas. Toutefois, le responsable ne peut pas se soustraire à l'obligation d'informer en faisant valoir qu'il ne sait pas exactement à quel client les données ont été volées. Une exception à l'obligation d'informer la personne concernée est, après tout, prévue pour les intérêts primordiaux des tiers, qui peuvent également être les intérêts des autorités à ce que l'enquête sur l'incident ne soit pas perturbée.

[167] Il est intéressant de noter qu'aucune des obligations d'annonce et d'information susmentionnées n'est assortie de **sanctions pénales** ; il en va autrement du RGPD. La motivation à signaler de manière effective chaque violation de la sécurité des données ne sera dès lors pas très grande. Le risque le plus important est probablement celui des réclamations des personnes concernées, notamment si elles se sont pas en mesure d'agir en temps utile parce que les informations leur ont été fournies trop tard ou de manière incomplète et qu'elles ne sont donc pas en mesure de se protéger pleinement contre un préjudice. Le droit suisse prévoit encore d'autres obligations d'annonce en cas de violations de la sécurité des données (p. ex. art. 29 al. 2 LFINMA, obligations d'annonce « ad hoc » selon le droit boursier).

D. Conseiller à la protection des données

[168] La nLPD a introduit la position de « **conseiller à la protection des données** ». Il est régi par l'art. 10 nLPD et peut être comparé au rôle du « délégué à la protection des données » prévu

140 FF 2017 6682.

aux art. 37 ss RGPD. Toutefois, pour de nombreux experts, cette disposition est une occasion manquée, car la nomination d'un conseiller à la protection des données n'est pas obligatoire et n'apporte aucun avantage pratique sur le plan juridique. En effet, sous l'ancien droit, la désignation d'un « délégué à la protection des données » (comparable dans sa conception) signifiait que les entreprises n'étaient plus obligées d'annoncer au PFPDT leurs collectes de données, qui devaient sinon être enregistrées[141].

[169] Dans la nLPD, le législateur ne prévoit qu'**une seule incitation à la nomination** d'un conseiller à la protection des données : imaginons un projet de traitement de données qui, malgré une AIPD et la définition de mesures, présente encore un « risque élevé ». Ce projet n'a plus besoin d'être soumis au PFPDT si le conseiller à la protection des données l'examine à sa place (art. 23 al. 4 nLPD). Cependant, l'expérience montre que de telles situations ne se produisent presque jamais (N 154).

[170] Toute personne qui, en tant que responsable du traitement, prend néanmoins la peine de désigner un tel conseiller à la protection des données doit **remplir plusieurs conditions** énumérées à l'art. 10 al. 2 et 3 nLPD. Le responsable du traitement doit : fournir au conseiller à la protection des données les moyens nécessaires pour qu'il puisse former et conseiller le responsable du traitement sur les questions de protection des données ; impliquer le conseiller à la protection des données dans ses processus de respect de la protection des données (ou lui confier une fonction de *« second line of defence »)* ; veiller à ce que le conseiller à la protection des données soit techniquement indépendant et ne soit pas lié par des instructions ; veiller à ce qu'il n'ait pas de conflit d'intérêts (c'est-à-dire que le conseiller à la protection des données ne peut pas exercer en parallèle des fonctions dans lesquelles il décide du traitement de données effectuées par le responsable du traitement ou dispose d'un intérêt à un tel traitement[142]) et le responsable du traitement doit avoir les compétences nécessaire ou à tout le moins avoir accès à ces compétences. En pratique, le conseiller à la protection des données sera donc probablement un prestataire de services externe, sauf dans le cas des grandes entreprises, ce qui est autorisé – par analogie avec les dispositions du RGPD. Les conflits d'intérêts seront sinon quasiment inévitables. Un **« délégué à la protection des données » d'un groupe de sociétés** peut également être un conseiller à la protection des données. Contrairement au représentant (N 172 ss), il n'est pas obligatoire que le conseiller à la protection des données se trouve en Suisse. Si un tel conseiller est désigné, il doit être annoncé au PFPDT et mentionné dans la déclaration de protection des données avec ses coordonnées (il n'est toutefois pas nécessaire de donner le nom de cette personne).

[171] Il faut s'attendre à ce que de nombreuses entreprises désignent une ou plusieurs personnes qui s'occuperont des questions de protection des données, car il n'y a pas d'autre option. Toutefois, ces personnes ne sont pas automatiquement considérées comme des conseillers à la protection des données et n'ont donc pas besoin d'être annoncées. Les exigences de l'art. 10 nLPD ne leur sont pas non plus applicables. Dans tous les cas, la violation de l'art. 10 nLPD n'est pas sanctionnée. Il est tout au plus concevable que le PFPDT ou un tribunal, dans un cas concret, parvienne à la conclusion qu'une entreprise aurait dû désigner un responsable de la protection des données compte tenu des circonstances particulières afin de garantir de manière adéquate la

141 Art. 11a LPD.

142 Cf. par exemple la décision de l'autorité belge de protection des données du 28 avril 2020 (AH-2019-0013), où le délégué à la protection des données a joué un rôle secondaire en tant que *compliance officer*, et à ce titre déterminait lui-même le traitement des données.

protection des données, et qu'il devrait l'ordonner sur la base des art. 7 et 8 nLPD. Toutefois, de tels situations devraient rester exceptionnelles.

E. Représentant suisse

[172] Le Parlement a introduit l'obligation pour certaines personnes privées responsables du traitement à l'étranger de désigner un **représentant en Suisse** (art. 14 ss nLPD). Il s'agit d'un mélange entre l'art. 27 RGPD (représentants de l'UE) et l'art. 3 al. 2 RGPD (application extraterritoriale du RGPD).

[173] Le nombre d'entreprises concernées devrait être faible. Les responsables du traitement domiciliés ou résidant à l'étranger ne doivent désigner un représentant en Suisse que (i) s'ils traitent les données personnelles de personnes en Suisse, (ii) s'ils offrent à ces personnes des biens ou des services ou observent leur comportement en Suisse, (iii) si le traitement de ces données est étendu et a lieu régulièrement, et (iv) si le traitement comporte un risque élevé pour la personnalité des personnes concernées. La plupart des entreprises considéreront que ce dernier critère n'est pas rempli, tout comme les AIPD ne conduisent pas régulièrement, dans la pratique, à la prise d'un risque élevé ou alors le traitement des données est ajusté jusqu'à ce qu'un tel risque n'existe plus. Le deuxième critère correspond en grande partie aux critères de l'art. 3 al. 2 RGPD et devrait probablement être interprété dans ce sens. Ainsi, soit un *ciblage* concret de la clientèle en Suisse est nécessaire, soit l'observation doit effectivement conduire à l'établissement d'un profil de la personne concernée ; le simple enregistrement de l'accès à un service en ligne ou à un site Internet ne suffit pas. Par conséquent, les fournisseurs de services tels que Facebook ou Google sont concernés, mais pas l'exploitant d'une boutique en ligne à l'étranger qui conserve ses données pour lui-même et établit le profil des utilisateurs à des fins de marketing dans une mesure usuelle. Bien entendu, tout responsable du traitement est libre de désigner volontairement un représentant suisse.

[174] Si un représentant est désigné conformément à l'art. 14 nLPD, il doit non seulement être **signalé au PFPDT**, mais il doit aussi être mentionné dans la déclaration de protection des données (art. 14 al. 2 et 3 nLPD). Il ne fait pas uniquement office de personne de contact pour les personnes concernées, mais également pour le PFPDT. Le représentant est légalement considéré comme un mandataire habilité à recevoir des notifications. C'est le sens et le but de cette disposition. Des dispositions analogues existent d'ailleurs aussi dans d'autres domaines du droit[143]. Le représentant doit conserver une copie du registre conformément à l'art. 12 nLPD et la communiquer au PFPDT sur demande de ce dernier ; cela ne s'applique toutefois pas au représentant désigné volontairement. Le représentant n'a pas d'autres obligations. Il n'est pas non plus responsable des éventuelles violations de la protection des données commises par le responsable du traitement. Il n'existe pas non plus de sanction pour la violation des art. 14 ss nLPD.

143 Par exemple lorsque des fournisseurs étrangers de services de télécommunications souhaitent utiliser les numéros de téléphone suisses à partir de 2021.

F. Codes de conduite

[175] Une innovation prometteuse de la nLPD est la possibilité d'établir des **codes de conduite**. Elle est régie par l'art. 11 nLPD. L'art. 40 RGPD contient une disposition similaire, mais plus stricte et beaucoup plus compliquée. Malheureusement, le législateur n'a pas non plus réussi à créer ici les incitations nécessaires à cette forme d'autorégulation. Alors que l'avant-projet prévoyait encore une forme de protection juridique en cas de respect d'un code de conduite, l'incitation juridique se limite désormais largement au fait que dans certains cas, il n'est plus nécessaire de mettre en œuvre une AIPD. A l'inverse, il n'y a aucune obligation de soumettre ces codes de conduite au PFPDT, bien que ce dernier ait souhaité que cela soit le cas[144].

[176] En termes de contenu, un code de conduite peut traiter chaque aspect de la LPD et ainsi apporter une forme de soutien dans son application. Il s'agirait par exemple d'expliquer quand il existe un « risque élevé », comment rendre les données suffisamment anonymes dans un secteur particulier, de modèles de déclaration de protection des données ou d'AIPD, d'une liste de cas dans lesquels l'intérêt du responsable de traitement est prédominant et qui iraient ainsi au-delà de l'art. 31 al. 2 nLPD, de périodes de conservation de certaines données ou de règles visant à garantir l'exportation de données personnelles vers un pays ne disposant pas d'une protection des données adéquate. Un code de conduite ne doit pas nécessairement être complet ; il peut se référer à un aspect particulier, ce qui devrait également être beaucoup plus facile à réaliser. Il ne doit pas non plus se limiter à la LPD. Toutefois, il doit être au moins aussi strict et plus spécifique que la LPD (et ne pas se contenter de la répéter) et il ne peut s'adresser qu'aux parties de l'organisation qu'il soumet au PFPDT. Les entreprises extérieures ne constituent toutefois pas un obstacle.

[177] Un code de conduite peut, mais ne doit pas, être soumis au PFPDT. Les personnes habilitées à le présenter sont les associations professionnelles ou économiques. Par analogie avec l'art. 89 CPC, il s'agit de toute organisation qui est autorisée par ses statuts à défendre les intérêts économiques de ses membres. A cet égard, les sociétés anonymes et les fondations ne disposent pas de membres. En revanche, les organisations de consommateurs ou les associations de personnes concernées ne peuvent soumettre de code de conduite au PFPDT.

[178] Si un code de conduite est soumis au PFPDT, ce dernier doit prendre position à son sujet. Le critère est ici **uniquement le respect de la LPD** et non une mise en conformité excessive, quand bien même le PFPDT pourrait le souhaiter. S'il veut proposer lui-même une alternative, il peut recourir à son propre instrument, à savoir la « recommandation de bonnes pratiques » prévue à l'art. 58 al. 1 let. g nLPD. Son avis ne constitue pas une décision[145], mais un acte matériel. Il doit être publié. En termes de contenu, il ne représente que son opinion actuelle, ce qui lui confère toutefois un poids considérable en pratique. Lors de la mise en place de ces recommandations, les justiciables pourront documenter leur respect de la LPD et démontrer le respect de leur devoir de diligence. Si un code de conduite est simultanément reconnu comme clause type de protection des données au sens de l'art. 16 al. 2 let. d nLPD, il peut également être utilisé pour **justifier l'exportation**. Le respect d'un code de conduite offre également une certaine protection de la bonne foi vis-à-vis du PFPDT, mais les exigences d'un tel code de conduite sont très élevées et

144 FF 2017 6654.

145 FF 2017 6654.

seront donc rarement remplies (p. ex. parce que le code n'est pas suffisamment précis ou que les faits sont légèrement différents, ou parce que la situation juridique ou les risques ont changé).

G. Certifications

[179] Les certifications existaient déjà dans l'ombre sous la LPD actuelle et il est peu probable que cela change malgré l'élargissement des possibilités de certification prévu à l'art. 13 nLPD. Auparavant, il était uniquement possible de certifier les entreprises pour certains ou l'ensemble de leurs processus et des mesures mis en place pour la protection des données (c'est ce que l'on entend par « systèmes » dans la nLPD). Désormais, les produits (à savoir le matériel et les logiciels) et les services peuvent également être certifiés **conformes à la LPD**. Dans la pratique, cela joue surtout un rôle lorsque la loi exige une certification[146], dans le cadre d'appels d'offres, ou lorsqu'un fournisseur entend pouvoir se démarquer. Le PFPDT aurait souhaité une obligation générale de certification pour les traitements à risque élevé. Le Conseil fédéral y a renoncé, dans la mesure où le RGPD ne l'exige pas non plus[147].

[180] Si une entreprise peut être certifiée, cela signifie qu'elle dispose d'un **système de gestion de la protection des données** (« SGPD ») **approprié** pour se conformer à la LPD, à savoir la gouvernance nécessaire au respect de la LPD. Cela ne signifie pas pour autant que les traitements de données, pris individuellement, sont effectués dans le respect de la loi. La manière dont les exigences en matière de certification des produits et des services seront conçues sera précisée dans le cadre de l'ordonnance qui doit encore être élaborée. En revanche, on ne peut pas déduire d'une certification que l'utilisation de ces produits ou services est automatiquement conforme aux règles de protection des données. En pratique, les certifications dans le domaine de la sécurité des données (p. ex. la norme ISO 27001) sont beaucoup plus importantes – même si elles ne sont pas mentionnées à l'art. 13 nLPD – car, sous certaines conditions, elles permettent de documenter l'adéquation des mesures prises par rapport à la sécurité des données. Parmi ces mesures, les normes ISO peuvent faire l'objet d'une certification conformément à l'art. 13 nLPD.

V. Mise en œuvre de la LPD

A. Par le PFPDT

[181] En raison des exigences légales européennes, l'application de la LPD par le PFPDT a été complètement repensée (également) dans le secteur privé. Le PFPDT ne fonctionne plus avec des « recommandations » adressées aux différents responsables du traitement des données, ce qui lui accordait une grande liberté de « sélection ». Il doit maintenant – comme toute autorité de surveillance – mener des procédures administratives ordinaires et **rendre des décisions** appropriées s'il souhaite intervenir. Bien que cela lui donne formellement plus de « pouvoir », il devra en même temps faire face à de plus grandes contraintes procédurales, cela signifie qu'il aura besoin de plus de ressources à l'avenir pour obtenir les mêmes résultats. Il est donc compréhensible que,

146 Selon l'art. 59a al. 6 de l'ordonnance sur l'assurance-maladie (OAMal ; RS 832.102), chaque point de collecte de données d'un assureur maladie de base doit être certifié.

147 FF 2017 6656.

contrairement à ses collègues de l'UE, il n'ait pas souhaité avoir la compétence nécessaire pour infliger des amendes aux responsables du traitement et aux sous-traitants fautifs. Cette compétence (et le travail qui l'accompagne) est du ressort des cantons (N 191).

[182] Conformément à l'art. 49 al. 1 nLPD, le PFPDT doit à l'avenir poursuivre **d'office** les violations des dispositions de la LPD. Chacun peut dénoncer de telles violations au PFPDT ; une déclaration dans la presse peut également suffire. Afin d'éviter de crouler sous les procédures, il peut (selon le principe d'opportunité) s'abstenir d'ouvrir une enquête dans le cas de violations « de peu d'importance » (al. 2). Il l'invoquera, par exemple, dans le cas d'annonces de violation de données, s'il est clair que la violation n'est pas grave ou que le responsable du traitement la maîtrise[148]. Il pourra également invoquer la possibilité de renoncer à l'ouverture d'une enquête lorsqu'il estime que des « recommandations » appropriées au responsable du traitement des données sont suffisantes pour rétablir une situation conforme au droit[149]. Dans ce cas, il peut mettre fin de manière anticipée à la procédure en prononçant un « **avertissement** » (art. 51 al. 5 nLPD). Cela devrait devenir la règle et contribuer à limiter les coûts pour toutes les parties concernées. En outre, il ne *doit* ouvrir une procédure que s'il existe des « indices suffisants » d'une violation de la protection des données (art. 49 al. 1 nLPD). Le message du Conseil fédéral ne mentionnait que des « indices ». Le fait que, selon l'art. 49 al. 1 nLPD, le PFPDT ne puisse ouvrir une procédure que dans le cas d'un *traitement de données* qui viole les règles de protection des données doit être interprété de manière large : le PFPDT peut également enquêter sur les personnes qui violent des mesures d'accompagnement et des droits des personnes concernées.

[183] Bien qu'une enquête soit généralement dirigée contre un responsable du traitement ou un sous-traitant, une procédure peut également être engagée **contre toute autre personne privée**. Le libellé de l'art. 49 al. 1 nLPD est ouvert sur ce point. On pourrait penser au représentant au sens de l'art. 14 nLPD. Le PFPDT ne peut pas contraindre des tiers à coopérer sur la base de l'art. 49 ou 50 nLPD ; ils sont toutefois soumis à l'obligation générale de témoigner et de coopérer conformément aux art. 15 et 17 de la Loi sur la procédure administrative (PA)[150].

[184] Tant qu'une procédure d'enquête n'est pas ouverte, les personnes privées ne sont pas tenues de fournir des informations au PFPDT. Elles seront souvent bien avisées de le faire quand même, si une affaire peut être réglée de cette façon dans le cadre d'une procédure préliminaire informelle. Une fois la procédure d'enquête ouverte, la PA s'applique (art. 52 al. 1 nLPD). **L'obtention d'informations par le PFPDT** se déroule en deux étapes :

a. Dans un premier temps, elle se fait par le biais d'une simple requête : les personnes privées interrogées – il ne doit pas nécessairement s'agir de personnes responsables ou de sous-traitants – sont tenues de **collaborer** conformément à l'art. 49 al. 3 nLPD, sous réserve du droit de refuser de témoigner. La collaboration peut être requise de manière informelle. Une partie n'est pas obligée de faire plus que de fournir des informations et des documents à ce stade.
b. Si cela n'aboutit pas ou n'est pas suffisant, l'art. 50 nLPD donne au PFPDT le pouvoir d'obtenir les informations et les renseignements nécessaires à l'enquête par le biais de **mesures**

148 Le message du Conseil Fédéral mentionne même l'exemple inoffensif d'une association qui envoie un e-mail à ses membres en omettant de cacher l'identité des destinataires (FF 2017 6706).

149 Dans ce sens également FF 2017 6706.

150 Loi fédérale sur la procédure administrative (PA) du 20 décembre 1968, RS 172.021.

de contrainte, le cas échéant avec l'aide de la police. Il ne devrait pas y avoir de véritables « *Dawn Raids* », c'est-à-dire des perquisitions inopinées d'un domicile : la compétence de recourir à des mesures de contrainte présuppose que le PFPDT ait d'abord tenté sans succès d'obtenir la collaboration des personnes concernées (art. 50 al. 1 nLPD).

[185] Le pouvoir du PFPDT d'ordonner des **mesures provisionnelles** a été supprimé de l'art. 50 nLPD par le Parlement[151] ; la PAelle-même ne le prévoit que pour la procédure de recours. La doctrine admet la possibilité de les ordonner également en procédure administrative. Cela doit également s'appliquer dans le cas présent – la suppression doit être considérée comme un oubli et non comme un silence qualifié.

[186] Si le PFPDT a constaté une violation des dispositions de la LPD en matière de protection des données, il peut rendre une décision correspondante (mais n'est pas obligé). S'il le fait, il dispose de pouvoirs étendus, limités par le principe de proportionnalité : il peut exiger la modification, la suspension ou la cessation du traitement des données, l'effacement des données personnelles traitées et la mise en œuvre des mesures d'accompagnement et des droits des personnes concernées (art. 51 al. 1 et 2 nLPD). Comme la **compétence pour ordonner des mesures** dépend de la violation de dispositions relatives à la protection des données, la LPD limite également cette compétence par ce biais ; ainsi, le PFPDT ne peut exiger que ce que la LPD permet de demander même sans son intervention. Il ne peut donc pas ordonner la communication d'informations s'il existe des motifs de refus, ni exiger une AIPD si les exigences de l'art. 22 al. 1 et 2 nLPD ne sont pas remplies. S'il veut imposer une consultation au sens de l'art. 23 nLPD ou la désignation d'un représentant suisse au sens de l'art. 14 nLPD, il doit établir que le traitement de données en question comporte un risque élevé malgré les mesures prises par les responsables du traitement, ou que les conditions de l'art. 14 nLPD sont remplies. A première vue, l'art. 51 al. 2 nLPD présente une particularité : il permet au PFPDT d'interdire la divulgation de données personnelles à l'étranger, et ce également en se fondant sur des dispositions d'autres lois fédérales. Toutefois, il doit également s'agir de dispositions visant (entre autres) la protection des données[152].

[187] Si une partie ne collabore pas de manière intentionnelle à une enquête du PFPDT comme exigé d'elle (de manière valable) ou si elle lui donne intentionnellement de faux renseignements, elle peut être punie d'une **amende** allant jusqu'à CHF 250'000 (art. 60 al. 2 nLPD). En cas de non-respect intentionnel d'une injonction du PFPDT au sens de l'art. 50 nLPD (p. ex. pour l'accès aux locaux), l'amende est la même (art. 63 nLPD). Même si seul l'art. 63 nLPD exige au préalable de menacer d'une amende, il doit en être de même pour l'art. 60 al. 2 nLPD. On ne voit pas pourquoi le seuil des amendes est plus bas en cas de non-respect d'une collaboration demandée de manière informelle que dans le cas d'une collaboration exigée dans une décision. Enfin, la même amende punit également le non-respect d'une mesure ordonnée ; cela signifie, bien entendu, que le prononcé de la mesure doit être suffisamment précis pour que les autorités cantonales de poursuite pénale puissent déterminer s'il a été respecté ou non. Dans le cadre des activités commerciales, l'amende est toujours infligée à la personne physique responsable (N 191).

151 Conseil national, BO 2019 N 1829 ss ; session d'automne 2019, 25 septembre 2019 ; Cf. même endroit : avis minoritaire du CN Minder selon lequel le PFPDT doit pouvoir ordonner des mesures provisionnelles (BO 2019 N 1823) ; Il faut noter que l'art. 44 du projet du Conseil fédéral est devenu l'art. 50 du texte révisé.

152 Il doit s'agir de dispositions qui règlent la communication de *données personnelles*, ce qui signifie que le législateur envisage des dispositions qui visent à protéger ces données et donc la personnalité des personnes concernées.

[188] Le destinataire de la décision du PFPDT peut **former un recours** contre la décision devant le Tribunal administratif fédéral, puis devant le Tribunal fédéral ; le PFPDT peut également porter la décision du Tribunal administratif devant le Tribunal fédéral (art. 52 al. 2 et 3 nLPD).

[189] Les personnes concernées, mais aussi d'éventuels tiers, n'ont pas la qualité de partie. Les personnes concernées doivent faire valoir leurs droits par la voie civile. En effet, les personnes concernées – si elles ont procédé à une dénonciation – ont le droit d'être informées des « suites » données à cette dénonciation et du « résultat » d'une enquête du PFPDT (art. 49 al. 4 nLPD). Il ne s'agit ainsi pas d'un droit de consulter le dossier. Les autres personnes concernées n'ont pas ce droit à l'information. Toutefois, le PFPDT contrôle en grande partie qui il souhaite informer sur ses affaires et comment (sous réserve de la protection des secrets d'affaires, de la protection de la personnalité des personnes concernées et de la proportionnalité). S'il ne peut pas fournir ces informations dans le cadre de l'art. 49 al. 4 nLPD, il peut se fonder sur l'art. 57 al. 2 nLPD, qui lui permet d'**informer le public** « de ses constatations et de ses décisions » lorsque l'intérêt général le commande. Il a déjà fait un vaste usage de cette compétence sous le droit actuel. Il convient également de noter qu'une fois la procédure terminée, le PFPDT peut encore accorder au public l'accès à ses documents en vertu de la **Loi sur la transparence** (LTrans)[153]. Il y accordera généralement un accès complet. Il convient donc de faire preuve de prudence quant aux documents qui lui sont communiqués au cours d'une enquête, dans la mesure où il existe une marge de manœuvre à cet égard.

[190] La nLPD contient désormais également des **dispositions relatives à l'assistance administrative**, y compris pour les pays étrangers (art. 55 nLPD). Elle permet désormais au PFPDT d'échanger ses conclusions également avec des autorités de protection des données étrangères, telles que celles de l'EEE, ou recevoir les informations nécessaires de leur part et les utiliser pour ses propres enquêtes. Toutefois, aucune application réciproque de mesures de contrainte n'est envisagée : les amendes ou autres mesures des autorités de protection des données de l'UE ne peuvent donc toujours pas être exécutées en Suisse. Le PFPDT devrait infliger des amendes ou d'autres mesures de son propre chef, ce qui n'est pas possible dans le premier cas. En revanche, il peut autoriser les autorités étrangères de protection des données à notifier elles-mêmes leurs décisions directement en Suisse, sans violer de ce fait l'art. 271 CP (art. 58 al. 3 nLPD).

B. Dispositions pénales

[191] Les dispositions pénales ont été considérablement élargies dans la nLPD : d'une part, un nombre considérablement plus important d'infractions est désormais punissable et, d'autre part, la fourchette des amendes a été portée de CHF 10 000 à CHF 250 000. Dans l'avant-projet, il était même de CHF 500 000. Cela peut sembler insignifiant par rapport au RGPD, qui prévoit une amende de 20 millions d'euros ou quatre pour cent du chiffre d'affaires annuel mondial total de l'exercice précédent. Toutefois, les amendes prévues par le RGPD sont infligées à l'entreprise, alors que les amendes suisses sont infligées **à la personne physique responsable**[154]. Selon l'opinion majoritaire, il n'est pas possible de s'assurer contre ce risque et l'entreprise ne peut pas payer

153 Loi fédérale sur le principe de la transparence dans l'administration du 17 décembre 2004, RS 152.3.

154 Cela se justifie par le fait que la procédure administrative suisse ne contient pas encore les garanties procédurales nécessaires en matière pénale, qui seraient requises pour infliger des amendes administratives comparables à celles du RGPD (FF 2017 6713 ss).

les amendes à la place de la personne physique[155]. Cela les rend en principe plus sévères que les amendes prévues par le RGPD, car pratiquement aucun salarié ne sera prêt à prendre un tel risque pour son employeur.

[192] Toutefois, la Suisse est loin derrière le RGPD à deux égards : d'une part, en Suisse, seule la violation intentionnelle de la LPD est punie et, d'autre part, le catalogue des infractions est beaucoup plus restreint que celui du RGPD. Alors que presque toutes les violations du RGPD sont passibles d'une amende, seules quelques dispositions de la nLPD sont concernées. La violation des principes de traitement n'est en elle-même pas plus punissable que la violation de la plupart des mesures d'accompagnement.

[193] Par ailleurs, les **autorités cantonales de poursuite pénale** sont responsables de l'application des dispositions pénales (art. 65 al. 1 nLPD), bien qu'elles n'aient généralement aucune expérience en matière de protection des données. Même si le PFPDT peut dénoncer des infractions et exercer les droits de la partie plaignante[156] (art. 65 al. 2 nLPD), il n'a pas le droit de déposer une plainte pénale – bien que la plupart des infractions soient des délits poursuivis sur plainte. On peut donc d'ores et déjà supposer que les amendes fondées sur les dispositions pénales des art. ss 60 nLPD seront l'exception en Suisse. Toutefois, on peut également supposer que les amendes créeront une pression psychologique dans les entreprises – en particulier au niveau de la direction – pour qu'elles respectent la protection des données.

[194] Selon l'art. 60 nLPD, comme sous l'ancien droit, la violation intentionnelle du **devoir d'informer** prévu aux art. 19 et 21 nLPD et certaines violations intentionnelles du **droit d'accès** prévu aux art. 25 ss nLPD par des personnes privées sont punissables. Pour plus de détails, voir N 92 et N 115. L'amende est désormais également de CHF 250 000. On peut supposer que la plupart des affaires pénales relevant de la LPD concerneront le droit d'accès, car c'est là que le risque de conflit entre les responsables du traitement et les personnes concernées est le plus élevé. La deuxième place est susceptible d'être accordée au devoir d'informer (par les consommateurs qui tentent ainsi d'agir contre les grandes entreprises) et aux transferts de données à l'étranger (dans les relations litigieuses). Les personnes concernées dans le cas d'espèce peuvent porter plainte au pénal. Il convient de noter que leur **droit de porter plainte** se prescrit par trois mois après la connaissance de l'auteur de l'infraction[157]. Étant donné que l'auteur de l'infraction est une personne physique qui était responsable de l'information en question ou de sa communication, et que cette personne physique ne sera généralement pas connue de la personne concernée, le délai pour déposer plainte ne jouera en principe aucun rôle.

[195] Le **responsable** du traitement peut faire partie de la direction (en raison de son obligation légale de veiller au respect de la LPD dans l'entreprise[158]), mais ce n'est pas obligatoire. Sans être un organe de la personne morale, un responsable du traitement peut également être poursuivi s'il dirige l'opération en cause[159], tel que le préposé à la protection des données de l'entreprise ou le

155 Vera Delnon/Bernhard Rüdy : in Basler Kommentar, Strafgesetzbuch II, 4e édition, Art. 305 CP, N 20, et les réf. cit. ; contre la qualification de l'entrave à l'exécution pénale : Damian K. Graf, Art. 305 N 9, in : Damian K. Graf (édit.), Annotierter Kommentar StGB, 1ère éd., Berne, 2020.

156 Il peut donc s'opposer aux décisions de classement et faire appel contre les jugements cantonaux. Toutefois, il ne devrait pas pouvoir faire appel contre les ordonnances pénales ou contre la quotité de la peine (FF 2017 6718 ss).

157 Art. 31 CP.

158 ATF 142 IV 315, c. 2 ss ; art. 29 CP ; art. 6 de la loi fédérale sur le droit pénal administratif (DPA ; RS 313.0).

159 Art. 29 let. d CP ; art. 6 al. 1 DPA.

conseiller juridique externe qui décide de la déclaration de protection des données ou des informations à fournir. S'il veut réduire son risque de responsabilité pénale, il doit laisser les décisions délicates à ses supérieurs ou à ses clients, car le **dol éventuel** est suffisant pour établir la responsabilité pénale. Dans un cas de dol éventuel, l'auteur estime que la réalisation de l'infraction est possible et s'en accommode ; il n'y a pas de dol éventuel mais une « négligence consciente » s'il considère également que la réalisation de l'infraction est possible mais qu'il compte sur le fait qu'elle ne se produira pas[160]. Contrairement aux propos rassurants du message du Conseil fédéral[161], la responsabilité pénale devrait donc affecter en premier lieu les organes exécutifs et non la direction. L'expérience montre qu'ils ne se pencheront pratiquement jamais sur les détails du devoir d'informer ou d'une demande de renseignements qui fondent la responsabilité pénale.

[196] De même, l'art. 64 nLPD, qui prévoit qu'en cas d'amendes allant jusqu'à CHF 50 000, c'est l'**entreprise elle-même** qui peut être condamnée à une **amende** à la place de la personne physique, a également peu de chances d'être efficace dans certains cas, même si les amendes ne dépassent normalement pas la limite de CHF 50 000. Cette disposition part du principe que les personnes responsables ne peuvent être identifiées qu'au prix d'un effort disproportionné. Cela ne sera toutefois que rarement le cas pour les infractions mentionnées ici.

[197] En outre, l'art. 61 nLPD définit trois « **obligations de diligence** », dont la violation intentionnelle par des personnes privées est également punissable d'une amende pouvant atteindre CHF 250 000. Ici aussi, l'infraction ne sera poursuivie que si les personnes concernées le demandent dans le cadre d'une plainte pénale. Les trois infractions sont les suivantes : violation des dispositions relatives à la communication de données personnelles à l'étranger (art. 16 ss nLPD), violation de certaines exigences imposées au responsable du traitement (art. 9 al. 1 et 2 nLPD) et non-respect des exigences minimales en matière de sécurité des données qui doivent encore être fixées par le Conseil fédéral dans l'ordonnance (art. 8 al. 3 nLPD). Pour plus de détails, voir N 79, N 60 et N 53.

C. Action civile

[198] La révision de la LPD n'apporte pas de changements significatifs dans le domaine de l'**exécution civile** des créances par les personnes concernées. Elles se basent sur l'art. 32 al. 2 nLPD, qui renvoie comme auparavant aux art. 28 ss CC. Il est toujours possible d'exiger des dommages-intérêts, un tort moral et la remise des gains, mais aussi des mesures concrètes relatives au traitement des données (telles que son interdiction totale ou partielle, l'interdiction de communiquer des données personnelles à des tiers ou encore l'effacement ou la rectification des données personnelles).

[199] Comme pour les litiges de droit du travail allant jusqu'à une valeur litigieuse de CHF 30 000, **aucun frais de justice** ne sera désormais perçu pour la procédure de conciliation et la procédure

160 Toutefois, si la probabilité de réalisation de l'infraction est suffisamment grande et que l'auteur a agi malgré tout, les tribunaux admettent que l'auteur n'avait pas d'autre choix que d'accepter la réalisation de l'infraction. Plus la probabilité de réalisation de l'infraction est grande et plus la violation du devoir de diligence est grave, plus il est admis que l'auteur s'est accommodé de la réalisation de l'infraction (ATF 130 IV 58).

161 FF 2017 6714.

au fond dans les litiges civils relevant de la LPD (art. 113 al. 2 let. g nCPC[162], art. 114 let. g nCPC). Il n'est également plus nécessaire de fournir des sûretés (art. 99 al. 3 let. d nCPC).

VI. Autres dispositions

A. Dispositions transitoires

[200] Il n'y a pas d'autres dispositions transitoires pertinentes concernant les nouvelles obligations de la LPD pour les particuliers. Le Parlement les a en grande partie supprimées durant les délibérations. La seule règle qui subsiste est celle selon laquelle l'art. 7 nLPD (Privacy by Design, Privacy by Default) et les art. 22 et 23 nLPD ne s'appliquent pas aux traitements de données qui ont commencé avant l'entrée en vigueur de la nLPD, à condition que la finalité du traitement reste inchangée et qu'aucune nouvelle donnée ne soit collectée. En raison de ces réserves, cette disposition transitoire est également sans pertinence en pratique.

[201] L'absence de période transitoire devrait être largement compensée, lorsque la nLPD entrera en vigueur en 2022, car dans la plupart des cas cette dernière n'exige pas d'adaptations fondamentales du traitement des données. Avant tout, la gouvernance doit être élargie. Les entreprises examineront en tout cas à un stade précoce si et comment elles veulent adapter leurs conditions générales et leurs déclarations de protection des données, par exemple en ce qui concerne le nouveau secret professionnel pour tous (cf. ci-après), les devoirs d'information modifiés, le transfert de données à l'étranger (également dans le cadre de « Schrems II », N 74) et la désignation de certains traitements de données sensibles. Dans le domaine de la sous-traitance, de nombreuses entreprises bénéficieront du fait que les contrats nécessaires à cet effet ont déjà été adaptés dans le cadre de l'introduction du RGPD. Souvent, seules des retouches sont nécessaires, mais cela nécessite également à tout le moins un réexamen des contrats.

B. Le secret professionnel pour tous

[202] L'une des innovations les plus notables de la nLPD est l'extension de l'ancien devoir de confidentialité à un **devoir général de discrétion pour tous les professionnels** (art. 62 nLPD)[163]. Bien que la précédente LPDcontenait un devoir de discrétion, son champ d'application était strictement limité aux données personnelles nécessaires sur le plan professionnel et aux profils de personnalité nécessitant une protection particulière. Désormais, sur plainte, toute personne qui divulgue intentionnellement des données personnelles secrètes dont elle a connaissance dans le cadre de son travail, qui nécessite de telles données personnelles, sera condamnée à une amende pouvant atteindre CHF 250 000, au lieu de CHF 10 000 auparavant. Les auxiliaires et les stagiaires sont également concernés par cette disposition. Le Conseil fédéral a justifié l'extension du devoir de discrétion à tous les types de données personnelles en invoquant, entres autres, « la propagation massive des téléphones intelligents »[164].

162 Cf. le texte de la nLPD soumis au vote final (N 4).

163 Art. 35 LPD.

164 FF 2017 6717.

[203] Le « petit secret professionnel » dans la LPD est également à mettre en lien avec le « grand » secret professionnel de l'art. 321 CP et le secret bancaire (art. 47 LB), dans la mesure où il est désormais question (comme pour ceux-ci) de **« révélation » en tant qu'acte**. On entend par là la divulgation des données en question à des personnes non autorisées. Par ailleurs, la notion de secret est la même que celle de l'art. 321 CP[165] : il doit s'agir d'informations qui ne sont pas largement connues et pour lesquelles le détenteur du secret a un intérêt manifeste à ce que le secret soit protégé[166]. L'art. 62 nLPD ne définit pas clairement qui est le détenteur du secret et cette question n'est pas abordée dans le message du Conseil fédéral. D'après le sens et le but de cette disposition et au vu de sa proximité avec l'art. 321 CP, voulue par le législateur, il doit s'agir de la personne qui a confié le secret au professionnel pour l'exercice de sa profession, tout comme dans l'art. 321 CP. En d'autres termes, comme dans le cas de l'art. 321 CP, la confiance que le client accorde à son avocat lorsqu'il lui confie des informations secrètes est protégée, de sorte que, conformément à l'art. 62 nLPD, le client doit être protégé dans sa confiance en son prestataire de services auquel il divulgue des données personnelles secrètes. L'art. 62 nLPD n'est donc pas, par essence, une norme de protection des données, même s'il ne s'applique qu'aux données *personnelles* et s'il figure dans la LPD. Bien que cette conclusion ne soit pas évidente, elle est capitale : il faut déterminer la personne dont le professionnel doit obtenir le consentement afin de pouvoir divulguer les données personnelles confidentielles à un tiers. Il s'agit dans ce cas uniquement du client, c'est-à-dire de la personne qui a confié ses données personnelles au professionnel à titre confidentiel. Là encore, le message du Conseil fédéral se réfère à l'art. 321 CP[167].

[204] En revanche, si l'art. 62 nLPD devait être qualifié de disposition de protection des données, cela signifierait notamment que toute personne concernée devrait consentir à la divulgation de ses données ou que l'autorisation de divulguer des données devrait se fonder sur les principes de la LPD : s'il existe un intérêt prépondérant à la divulgation, même des informations confidentielles pourraient être divulguées. A l'inverse, le consentement du client ne serait pas suffisant si les informations concernaient également d'autres personnes. Dans ces cas, la violation des principes de traitement serait sanctionnée par le droit pénal par des moyens détournés, bien qu'il n'existe pas de relation de confiance entre ces tiers et le professionnel et que ce dernier ne soit souvent pas en mesure (et n'ait pas le droit) de se poser la question. Un conseiller juridique pourrait ainsi être sanctionné pour violation du secret professionnel s'il divulgue des données personnelles au nom de son client mais contre la volonté de la partie adverse[168]. On peut supposer que telle n'est pas l'intention du législateur. L'affirmation inverse, soit le fait que l'art. 62 nLPD ne permette pas de poursuivre celui qui divulgue des données de manière *autorisée* au regard de la protection des données, ne peut pas être admise sans réserve sous cette forme. Quoi qu'il en soit, dans la

165 FF 2017 6717.

166 Niklaus Oberholzer, in : Basler Kommentar, Strafgesetzbuch II, 4e édition, art. 321 CP, N 14.

167 FF 2017 6717, qui prévoit que les règles générales et les principes développés par la jurisprudence et la doctrine dans le cadre de l'art. 321 ch. 2 CP doivent s'appliquer *mutatis mutandis*. Cela signifierait qu'à côté du consentement du bénéficiaire, une autorisation de l'autorité supérieure ou de l'autorité de surveillance permettrait également la divulgation. Toutefois, le message du Conseil fédéral laisse ouverte la question de savoir de quelle autorité il devrait s'agir.

168 Dans cet exemple, on a choisi un non-avocat qui n'est pas couvert par l'art. 321 CC, afin que la question de la concurrence entre ces deux normes ne se pose pas. Toutefois, étant donné que l'art. 321 CP ne protège de toute façon que le client ou la confiance dans l'avocat et non la partie adverse, l'exemple pourrait également fonctionner avec un avocat.

pratique, il n'y a que très peu de cas concevables dans lesquels cette dernière affirmation ne serait finalement pas applicable, car la LPD protège également la confiance du détenteur du secret, du moins en ce qui concerne ses données[169].

[205] Contrairement à l'art. 321 CP, l'art. 62 nLPD n'est plus un délit propre : ***tout* travailleur salarié** qui a connaissance de données personnelles dont il a besoin pour son travail est soumis au secret professionnel. Il s'agit d'une réglementation extrêmement large et – même en comparaison internationale – étonnamment stricte. Bien que les employés soient déjà tenus de garder le secret en vertu de l'art. 321a al. 4 CO, celui-ci protège les secrets d'affaires et de fabrication de l'*employeur et* non les secrets de ses clients – ou tout au plus indirectement. Désormais, ils sont également tenus de respecter le secret professionnel vis-à-vis des clients de l'employeur.

[206] Le champ d'application exact de cette norme ne peut pas encore être déterminé avec précision. Les secteurs qui traitent régulièrement des informations confidentielles mais qui n'étaient auparavant pas soumis au secret professionnel auront un intérêt à adapter leurs conditions générales pour éviter le risque de responsabilité pénale si des données relatives à leurs clients, bien que peu diffusées, sont néanmoins échangées avec des tiers. Cela peut affecter un assureur privé tout autant que l'exploitant d'une boutique en ligne ; tous deux n'étaient auparavant soumis à aucune obligation de confidentialité qui serait sanctionnée par le droit pénal. Toutefois, il convient également de noter que toutes les informations qu'une entreprise reçoit de ses clients ne peuvent pas être qualifiées de confidentielles. En outre, même dans le cas d'une information qui est secrète en soi, il convient de distinguer qui fait partie du cercle de ceux à qui l'information peut néanmoins être divulguée : si un assureur n'est sans doute pas autorisé à publier sur son site Internet les documents concernant le sinistre d'un client, leur communication à un coassureur ne constituera pas une révélation punissable, même si les conditions d'assurance ne prévoient pas de dérogation expresse à cet égard. Dans de tels cas, premièrement, il n'existe généralement aucun intérêt digne de protection qui empêcherait la divulgation et, deuxièmement, l'inclusion des coassureurs sera normalement au moins implicitement acceptée – et donc aussi l'autorisation de leur fournir les informations nécessaires. Comme dans le cas de l'art. 321 CP, l'obligation de secret ne peut s'étendre que dans la relation entre le maître du secret et le détenteur du secret. Le fait de mentionner la divulgation des données dans les déclarations de protection des données contribuera également à la réduction des risques. Bien que cela ne constitue pas nécessairement une dérogation en tant que telle, le fait qu'un client ait confié des données au prestataire de services en ayant connaissance de leur utilisation prévue peut affecter l'intérêt reconnaissable au maintien du secret s'agissant de cette utilisation. En tout état de cause, tout échange nécessaire à l'exécution du contrat ou prévu par celui-ci doit être autorisé en vertu de l'art. 62 nLPD, sans exception. Si une divulgation de données ne répond pas à ces critères, mais qu'il doit être clair pour le client qu'elle aura lieu et que celui-ci confie ses données à son fournisseur de services en tout connaissance de cause, il n'y a pas d'abus de confiance ou d'intérêt au secret et donc, à nouveau, aucune violation de l'art. 62 nLPD. Les personnes qui souhaitent tout de même se protéger peuvent compléter la référence à leur déclaration de protection des données dans leurs conditions générales en indiquant qu'elles se réservent le droit de divulguer les données qui y sont

169 En théorie, il s'agirait d'un cas où le client de la personne soumise au secret interdit une divulgation, mais où celle-ci semble néanmoins justifiée du point de vue de la protection des données en raison d'intérêts prépondérants. Ces intérêts devraient cependant être à ce point prépondérants qu'ils pourraient également constituer un motif justificatif dans le cadre de l'art. 321 CP.

mentionnées[170]. Les règles concernant les clauses inhabituelles et ambiguës doivent néanmoins être respectées. Une telle réserve n'est donc pas un « laissez-passer » pour toute divulgation de données. Plus les données sont sensibles, plus il faut prendre de précautions.

C. Usurpation d'identité

[207] En réponse à une motion adoptée par le Parlement[171], la révision de la LPD a également été utilisée pour introduire une nouvelle infraction pénale contre l'usurpation d'identité. Selon l'art. 179*decies* du code pénal révisé (nCP)[172], toute personne qui **utilise l'identité d'une autre personne sans son consentement** dans le dessein de lui nuire ou de se procurer un avantage illicite pour elle-même ou pour un tiers sera désormais punie, sur plainte, d'une peine privative de liberté pouvant aller jusqu'à un an. Le champ d'application de la norme est très large : par « identité » d'une personne, on entend non seulement son nom, mais aussi d'autres caractéristiques telles que sa photo, son numéro de compte, son nom d'utilisateur ou son *nickname*, son adresse Internet ou encore la combinaison de caractéristiques qui permettent d'identifier une personne déterminée[173]. Ainsi, cette norme concerne notamment la personne qui utilise le compte en ligne d'un tiers, tout comme la personne qui ouvre un compte au nom d'un tiers ou qui apparaît sous le nom d'un tiers. Jusqu'à présent, il n'était souvent pas possible d'appréhender de tels cas au moyen du droit pénal, ou du moins de protéger la personne dont l'identité a été utilisée (p. ex. pour une escroquerie).

[208] L'utilisation d'une identité étrangère par pure exubérance ou à titre de plaisanterie n'entre pas dans le champ d'application de cette disposition[174]. L'auteur doit **agir dans l'intention de causer un dommage ou de tirer un avantage** (l'intention de causer de graves ennuis chez la personne concernée devrait suffire[175]). L'utilisation d'identités inventées n'entre pas non plus en compte. Il en va de même du cas où une personne utilise des éléments d'identification d'une autre personne mais n'affirme pas son identité (p. ex. la représentation sur scène d'un humoriste utilisant un masque à l'effigie d'un politicien). Selon la nLPD, cela constitue « seulement » une violation de la personnalité, si tant est qu'il y en ait une.

David Rosenthal, lic. iur., associé, VISCHER AG, Zurich, chargé de cours à l'ETH Zurich et à l'Université de Bâle.

Traduit [et adapté] par Samira Studer et Alexandre Lombard. Texte original : https://jusletter.weblaw.ch/juslissues/2020/1045/das-neue-datenschutz_0e89d89706.html__ONCE

170 Exemple : « Pour plus d'informations sur la protection des données, y compris les divulgations de données que nous nous réservons le droit de faire, veuillez consulter notre déclaration de protection de données [lien] ».

171 CE Comte, motion du 21 mars 2014, n° 14.3288.

172 Cf. le texte de la nLPD soumis au vote final (N 4).

173 Cf. FF 2017 6741.

174 FF 2017 6741.

175 FF 2017 6742.