LE TRAITEMENT DE DONNÉES PERSONNELLES SOUS L'ANGLE DE LA (NOUVELLE) LOI FÉDÉRALE SUR LA PROTECTION DES DONNÉES DU 25 SEPTEMBRE 2020

par

Sylvain MÉTILLE

Professeur associé à l'Université, avocat

Tiré à part de la Semaine Judiciaire 2021 II 1 ss

LE TRAITEMENT DE DONNÉES PERSONNELLES SOUS L'ANGLE DE LA (NOUVELLE) LOI FÉDÉRALE SUR LA PROTECTION DES DONNÉES DU 25 SEPTEMBRE 2020

par

Sylvain MÉTILLE*
Professeur associé à l'Université,
avocat

I. INTRODUCTION

A. Le contexte

La révision totale de la Loi fédérale sur la protection des données est un trop long projet qui a débuté en décembre 2011 avec l'adoption par le Conseil fédéral d'un rapport sur l'évaluation de l'aLPD[1] et un mandat pour le Département fédéral de justice et police (DFJP) d'examiner l'opportunité de renforcer la législation en matière de protection des données[2]. La révision visait deux buts : la mise à jour de l'aLPD de 1992[3] et la reprise, dans le cadre de l'Acquis de Schengen, de la Directive (UE) 2016/680 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel à des fins de

* L'auteur tient à remercier chaleureusement M. LIVIO DI TRIA, assistant-doctorant à la Faculté de droit, des sciences criminelles et d'administration publique de l'Université de Lausanne pour son aide précieuse dans la rédaction de ce texte.

1 Pour faciliter la lecture, la Loi fédérale sur la protection des données du 19 juin 1992 (telle qu'en vigueur au 1er janvier 2021) est abrégée aLPD, alors que la Loi fédérale (révisée) sur la protection des données du 25 septembre 2020 est abrégée nLPD. L'avant-projet de révision totale de la Loi fédérale sur la protection des données mis en consultation le 21 décembre 2016 est abrégé AP-LPD et le projet publié par le Conseil fédéral le 15 septembre 2017 est abrégé P-LPD.

2 FF 2017 6567-6568.

3 Même si elle avait déjà subi quelques mises à jour. Voir notamment MEIER, N. 219 ss.

prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales.

L'avant-projet de révision totale de la nLPD a été mis en consultation le 21 décembre 2016[4] et l'on pouvait encore, un peu naïvement, espérer une entrée en vigueur alignée sur l'entrée en application du Règlement général de protection des données de l'UE (RGPD)[5] le 25 mai 2018. C'était sans compter les 3573 pages de commentaires formulés pendant la consultation[6] et les difficultés qui seront rencontrées au Parlement. Le projet de loi est publié par le Conseil fédéral du 15 septembre 2017[7]. La Commission des institutions politiques du Conseil national (CIP-N) a ensuite décidé de diviser le projet entre l'adaptation nécessaire à la Directive 2016/680 et la mise à jour autonome de la nLPD[8]. Cette décision a ensuite été confirmée par le Conseil national[9], obligeant le Conseil fédéral à présenter une nouvelle Loi fédérale sur la protection des données Schengen (LPDS) dont le champ d'application est principalement limité au traitement de données personnelles par des organes fédéraux à des fins de prévention et d'élucidation des infractions pénales, de poursuites en la matière ou d'exécution de sanctions pénales dans le cadre de la mise en œuvre de l'acquis de Schengen[10]. Entrée en vigueur le 1er mars 2019, la LPDS sera abrogée avec l'entrée en vigueur de la nLPD (art. 68 nLPD). La discussion de la nLPD a été très mouvementée et il a fallu recourir à une séance de conciliation pour que les deux chambres puissent finalement adopter le texte final le 25 septembre 2020.

La date d'entrée en vigueur n'a pas encore été fixée mais elle est tributaire de la rédaction de l'ordonnance, qui fait l'objet d'une consultation interne début 2021. Une consultation externe suivra au printemps,

---

4 https://www.bj.admin.ch/bj/fr/home/staat/gesetzgebung/datenschutzstaerkung.html (consulté 01.02.2021).

5 Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (Règlement général sur la protection des données), JO 2016 L 119, 8.

6 https://www.bj.admin.ch/bj/fr/home/staat/gesetzgebung/datenschutzstaerkung.html (consulté le 01.02.2021). Nous renvoyons ici aux bulletins officiels de l'objet 17.059 « Loi sur la protection des données. Révision totale et modification d'autres lois fédérales ». Les bulletins officiels sont sur le site web de l'Assemblée fédérale, à l'adresse suivante : https://www.parlament.ch/fr/ratsbetrieb/suche-amtliches-bulletin#k=PdAffairId:20170059 (consulté le 01.02.2021).

7 https://www.bj.admin.ch/bj/fr/home/staat/gesetzgebung/datenschutzstaerkung.html (consulté 01.02.2021).

8 https://www.parlament.ch/fr/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20170059 (consulté le 01.02.2021)

9 *Ibidem.*

10 Art. 1 et 2 LPDS.

mais une entrée en vigueur de la nLPD avant le 1er juin 2022 semble déjà improbable. À noter néanmoins que la nLPD sera entièrement applicable dès son entrée en vigueur et qu'aucune période de grâce n'est prévue[11]. Elle n'a pas non plus d'effet rétroactif, ce qui signifie qu'une information ne sera pas due en application de l'art. 19 nLPD si les données ont été collectées avant l'entrée en vigueur de la nLPD[12] Un consentement obtenu valablement selon l'aLPD continuera à être valable et les principes de protection des données dès la conception et par défaut, ainsi que l'analyse d'impact préalable ne seront pas applicables aux traitements qui ont débuté sous l'aLPD (art. 69 nLPD) pour autant que les finalités du traitement restent inchangées et que de nouvelles données ne sont pas collectées.

B. Les principales différences

La nLPD est plus une évolution ou une mise à jour qu'une révolution, le manque d'ambition du Conseil fédéral et la difficulté des chambres fédérales à se mettre d'accord n'ayant pas permis de renforcer sérieusement les pouvoirs de l'autorité de contrôle en matière de protection des données (PFPDT)[13], ni d'introduire de vraies sanctions administratives ou de moyens d'action collectifs.

La nLPD continue donc à s'appliquer à l'administration fédérale et aux privés qui traitent des données personnelles, et elle reprend les principes existants. S'agissant du traitement par des privés, il n'est toujours pas nécessaire d'avoir un motif justificatif (comme le consentement) pour traiter des données personnelles[14], mais c'est seulement lorsqu'il y a une atteinte à la personnalité (présumée dans les cas énumérés à l'art. 30 al. 2 nLPD, notamment la violation des principes), que le responsable du traitement doit se réfugier derrière un motif justificatif (art. 31 nLPD) pour que le traitement ne soit pas illicite.

Au niveau de la terminologie et du champ d'application, la nLPD ne s'applique plus aux données des personnes morales, le maître du fichier devient le responsable du traitement, et la notion statique de profil de la personnalité est supprimée au profit de celles, dynamiques, de profilage[15]

---

11 Contrairement au RGPD entré en vigueur le 24 mai 2016 mais applicable seulement à partir du 25 mai 2018 (art. 99 *RGPD*).

12 L'art. 19 nLPD prévoit une obligation d'informer de la collecte, pas de tout traitement.

13 Préposé fédéral à la protection des données et à la transparence.

14 Contrairement à ce que prévoient les art. 6 et 9 RGPD. Voir également ROSENTHAL, N. 7 s.

15 La définition du profilage aurait dû être alignée sur celle du droit européen (FF 2017 6601 et 6641 s). Les parlementaires semblent toutefois considérer que la notion de profilage est égale à celle de profil de personnalité (voir BO 2020 N. 139 ss).

et profilage à risque élevé. La nLPD introduit son lot de nouvelles obligations pour le responsable du traitement, comme l'information étendue y compris la mention des pays vers lesquels les données sont exportées, le registre des activités de traitement, l'analyse d'impact et la consultation préalable, l'annonce des violations de la sécurité, la protection des données dès la conception et par défaut, ainsi que le représentant en Suisse pour les responsables du traitement étranger. De nouveaux droits sont aussi reconnus pour la personne concernée, en particulier le droit à la portabilité[16] et le droit de faire revoir une décision individuelle automatisée par une personne physique.

II. LE CHAMP D'APPLICATION

A. Des données personnelles…

La nLPD s'applique au traitement de données personnelles[17] (art. 2 al. 1 nLPD). Contrairement à l'aLPD, les données de personnes morales ne sont plus protégées par la nLPD. La Suisse s'aligne ainsi sur les autres pays, ce qui devrait faciliter grandement le transfert de données à l'étranger[18]. Les personnes morales peuvent continuer à invoquer la protection générale de leur personnalité garantie par les art. 28 ss du CC[19].

La notion de données personnelles est large et inclut toutes les informations concernant une personne physique identifiée ou identifiable (art. 4 nLPD)[20]. Une personne est identifiée lorsque l'on sait de qui il s'agit. Elle est identifiable lorsqu'elle peut être identifiée, directement ou indirectement, sur la base d'un ou plusieurs éléments. Un nom, une adresse électronique, un numéro de téléphone, une adresse IP[21], un numéro AVS, une empreinte digitale, une adresse ou une date de naissance sont des données personnelles.

---

16 Appelé droit à la remise ou à la transmission des données personnelles.

17 Dans ce contexte, on parle aussi souvent simplement de données.

18 En particulier vers les pays offrant un niveau de protection adéquat pour les personnes physiques.

19 Cette modification a néanmoins eu un fort impact légistique pour le secteur public. En effet, les bases légales qui permettent le traitement de données personnelles ne permettent plus que le traitement de données de personnes physiques, alors que les personnes morales bénéficient de la protection de la sphère privée. De nombreuses lois ont donc dû être complétées (FF 2017 6595 et FF 2017 6632).

20 Le RGPD et certaines lois cantonales parlent plutôt de données à caractère personnel, sans que cela n'ait de conséquence pratique. Sur la notion de données personnelles, voir notamment ROSENTHAL, N. 19 ss ; CELLINA, N. 131 ss ; MEIER, N. 414 ss ; ROSSI.

21 MEIER, N. 446 et 447 ; ATF 136 II 508, c. 3.5 ; Arrêt CJUE Patrick Breyer c. Bundesrepublik Deutschland, C-582/14 du 19 octobre 2016, par. 49.

Les données pseudonymes[22] sont des données personnelles puisque la personne demeure identifiable. Si ce n'est pas le cas, on parlera de données anonymes. Les données anonymes ne sont pas soumises à la nLPD. Une possibilité purement théorique qu'une personne soit identifiée n'est pas suffisante. La possibilité d'identifier la personne concernée doit s'apprécier de façon relative, soit selon le point de vue de l'intéressé. Des données pseudonymes constituent des données personnelles seulement du point de vue de celui qui détient la table de concordance[23] ou de celui qui pourrait réidentifier la personne en mettant en œuvre des moyens raisonnables[24]. Ne seraient pas raisonnables des moyens interdits par la loi ou irréalisables en pratique (ou au prix d'efforts démesurés en termes de temps, de coût et de main-d'œuvre).

L'art. 5 let. c nLPD prévoit que certaines données personnelles sont sensibles. C'est le cas des données sur les opinions ou les activités religieuses, philosophiques, politiques ou syndicales (art. 5 let. c ch. 1 nLPD) ; des données sur la santé, la sphère intime ou l'origine raciale ou ethnique (art. 5 let. ch. 2 nLPD) ; des données génétiques (art. 5 let. c ch. 3 nLPD) ; des données biométriques identifiant une personne physique de manière univoque (art. 5 let. c ch. 4 nLPD)[25] ; des données sur des poursuites ou sanctions pénales et administratives (art. 5 let. c ch. 5 nLPD) ; ainsi que des données sur des mesures d'aide sociale (art. 5 let. c ch. 6 nLPD).

Contrairement à ce que prévoit le RGPD[26], le traitement de données sensibles n'est pas interdit par principe, mais il demande une plus grande prudence et peut déclencher quelques obligations supplémentaires comme une analyse d'impact préalable en cas de traitement à grande échelle (art. 22 al. 2 let. a nLPD) ou un consentement pour pouvoir les traiter dans le but d'évaluer la solvabilité[27]. Si un consentement est requis, il doit être exprès (art. 6 al. 7 nLPD) et finalement lorsque les données sont traitées par un organe fédéral, la base légale doit être formelle et pas simplement matérielle (art. 34 al. 2 nLPD).

---

22 Le RGPD définit la pseudonymisation comme le traitement de données personnelles de telle façon que celles-ci ne puissent plus être attribuées à une personne concernée précise sans avoir recours à des informations supplémentaires, pour autant que ces informations supplémentaires soient conservées séparément et soumises à des mesures techniques et organisationnelles afin de garantir que les données personnelles ne sont pas attribuées à une personne physique identifiée ou identifiable.

23 TF 4A_365/2017 du 26 février 2018, c. 5.1.1.

24 FF 2017 6639-6640 ; Arrêt CJUE Patrick Breyer c. Bundesrepublik Deutschland, C-582/14 du 19 octobre 2016, par. 42-46.

25 Les données génétiques et les données biométriques ne figuraient pas dans l'aLPD.

26 Art. 9 RGPD.

27 Art. 31 al. 2 let. c nLPD.

B. … traitées par des privés et organes fédéraux…

La nLPD s'applique au traitement de données personnelles par des personnes privées (physiques ou morales) ou des organes fédéraux (art. 2 al. 1 nLPD). La nLPD a en effet la particularité de concrétiser tant la protection de la personnalité du droit privé au sens des art. 28 ss CC, que la protection de la sphère privée du droit public au sens de l'art. 13 Cst.

La notion de traitement est aussi très large et recouvre toute opération relative à des données personnelles, indépendamment des moyens et procédés utilisés (art. 5 let. d nLPD). Cela inclut par exemple la collecte, l'enregistrement, la conservation, l'utilisation, la modification, la communication, l'archivage, l'effacement ou la destruction de données[28].

La nLPD s'applique de la même manière à toutes les personnes privées qui traitent des données, à l'exception des traitements effectués par une personne physique pour un usage exclusivement personnel qui ne sont pas soumis à la nLPD (art. 2 al. 2 let. a nLPD)[29].

Par organe fédéral, il faut comprendre non seulement une autorité ou un service fédéral, mais également une personne privée chargée d'une tâche publique de la Confédération (art. 5 let. i nLPD)[30]. Le traitement de données personnelles effectué par les Chambres fédérales et les commissions parlementaires dans le cadre de leurs délibérations (art. 2 al. 2 let. b nLPD) ou par les bénéficiaires institutionnels qui jouissent en Suisse de l'immunité de juridiction (art. 2 al. 2 let. c nLPD) ne sont pas soumis à la nLPD[31]. Quant au traitement de données par les autorités cantonales, il n'est pas soumis à la nLPD, mais est régi par le droit cantonal[32].

La nLPD ne s'applique pas non plus au traitement de données personnelles effectué dans le cadre de procédures devant des tribunaux ou dans le cadre de procédures régies par les dispositions de la procédure fédérale (art. 2 al. 3 nLPD)[33]. C'est le droit de procédure qui s'applique, sauf pour les procédures administratives fédérales de première instance.

Géographiquement, l'art. 3 nLPD introduit par le Conseil national précise que la nLPD s'applique aussi aux états de fait qui se sont

---

28 MEIER, N. 519 ss ; BSK DSG-BLECHTA, art. 3 N. 71 ss.

29 MEIER N. 378 SS ; BSK DSG-LAMBROU / KUNG, art. 2 N. 21-22.

30 MEIER, N. 364 ; BSK DSG-BLECHTA, art. 3 N. 82-86. Par exemple, est une personne privée chargée d'une tâche publique de la Confédération la caisse de compensation AVS privée conformément à l'art. 53 de la Loi fédérale du 20 décembre 1946 sur l'assurance-vieillesse et survivants.

31 BSK DSG-LAMBROU / KUNZ, art. 2 N. 23 ss.

32 MEIER, N. 356. Sur le traitement de données personnelles par un organe fédéral, voir en particulier BELSER / EPINEY / WALDMANN.

33 MEIER, N. 386 ; BSK DSG-LAMBROU / KUNZ, art. 2 N. 26 ss.

produits à l'étranger, mais qui déploient des effets en Suisse[34]. Cela codifie la jurisprudence du Tribunal fédéral rendue dans l'affaire *« Google Street View »* où il avait été confirmé que des images prises en Suisse et publiées d'une façon qui permet d'y accéder en Suisse également ont un lien prépondérant avec la Suisse, même si elles sont traitées à l'étranger et ne sont pas mises en ligne directement depuis la Suisse[35].

III. LES ACTEURS

On distingue traditionnellement la personne concernée, le responsable du traitement et le sous-traitant[36].

La personne concernée est la personne physique, identifiée ou identifiable, dont les données personnelles font l'objet d'un traitement (art. 5 let. b nLPD). C'est sa personnalité que la nLPD veut protéger (art. 1 nLPD).

Le responsable du traitement est la personne privée ou l'organe fédéral qui, seul ou conjointement avec d'autres[37], détermine les finalités et les moyens du traitement de données personnelles (art. 5 let. j nLPD). La notion de « responsable du traitement » remplace ainsi la notion de « maître du fichier » de l'art. 3 let. i aLPD. Ce changement terminologique s'explique notamment en raison de la volonté du législateur de s'aligner une notion plus largement reconnue[38], ainsi qu'en raison de la suppression de la notion de « fichier » tel que prévu à l'art. 3 let. g aLPD.

Le sous-traitant est la personne privée ou l'organe fédéral qui traite des données personnelles pour le compte et selon les instructions du responsable du traitement (art. 5 let. k nLPD).

---

34 Voir également COMITÉ EUROPÉEN DE LA PROTECTION DES DONNÉES, Lignes directrices 3/2018 relatives au champ d'application territorial du RGPD (article 3), Version 2.0 du 12 novembre 2019.

35 ATF 138 II 346, c. 3.3.

36 Dans la terminologie de la protection des données, le sous-traitant n'est pas un tiers. La notion de destinataire recouvre en revanche tant le tiers que le sous-traitant à qui sont communiquées des données. Sur ces notions, voir COMITÉ EUROPÉEN DE LA PROTECTION DES DONNÉES, Guidelines 07/2020 on the concepts of controller and processor in the GDPR du 7 septembre 2020

37 La nLPD ne prévoit pas de dispositions particulières concernant les responsables du traitement conjoint, si ce n'est un renvoi à l'ordonnance les procédures de contrôle et les responsabilités lorsque les données sont traitées conjointement par un organe fédéral et un autre organe fédéral ou cantonal ou une personne privée (art. 33 nLPD). On pourra s'inspirer de l'art. 26 RGPD qui prévoit que les responsables conjoints du traitement doivent définir de manière transparente leurs obligations respectives, notamment en ce qui concerne l'exercice des droits de la personne concernée et leurs obligations d'information.

38 Notamment dans la plupart des droits cantonaux, ainsi qu'en droit européen et international (FF 2017 6643).

Le destinataire est la personne privée ou l'organe fédéral à qui des données sont transférées. Il peut intervenir en qualité de tiers (responsable du traitement indépendant) ou de sous-traitant[39].

IV. Les principes

A. La bonne foi

Tout traitement de données personnelles doit être effectué conformément au principe de la bonne foi (art. 6 al. 2 nLPD). Si le principe de la bonne foi est un principe général de l'ordre juridique suisse (art. 2 CC), celui-ci se traduit, dans le domaine de la protection des données, par le fait qu'aucune donnée ne doit être traitée à l'insu de la personne concernée ou contre sa volonté[40]. Celui qui, lors de la collecte des données, laisse croire à la personne concernée que toutes les données sont obligatoires alors que certaines sont facultatives, viole le principe de la bonne foi.

B. La licéité

L'art. 6 al. 1 nLPD prévoit que tout traitement de données personnelles doit être licite.

La notion de licéité doit se comprendre ici comme l'absence de violation d'une norme impérative du droit de la protection des données ou d'une norme visant à protéger la personnalité[41], par exemple obtenir ou traiter des données en violation d'un secret[42]. Dans le cadre d'un arrêt récent opposant le PFPDT à la société suisse d'assurances Helsana, le Tribunal administratif fédéral a précisé que le principe de licéité était violé seulement lorsqu'une norme légale visant la protection de la personnalité était violée, et pas n'importe quelle norme légale[43].

Pour les organes fédéraux, il est important de souligner également l'exigence de la base légale : des données personnelles ne peuvent être

---

39 Meier, N. 612 ss.

40 Meier, N. 644 ss.

41 Meier, N. 637 ss ; BSK DSG-Lambrou / Steiner, art. 4 N. 5 ss.

42 Art. 320 ss CP et 47 LB.

43 TAF A-3548/2018 du 19 mars 2019, c. 5.4.4. Dans le cadre de cette affaire, le Tribunal administratif fédéral est arrivé à la conclusion que les art. 61 ss de la Loi fédérale du 18 mars sur l'assurance-maladie ne visent pas à protéger la personnalité des personnes assurées, ce faisant leur possible violation est sans effet sur la protection des données.

traitées que s'il existe une base légale (art. 34 al. 1 nLPD)[44]. Elle doit même être formelle s'il s'agit de données sensibles, d'un profilage ou qu'il y a un risque de porter gravement atteinte aux droits fondamentaux de la personne concernée (art. 34 al. 2 nLPD). Une base légale matérielle peut néanmoins suffire si le traitement est indispensable à l'accomplissement d'une tâche définie dans une loi formelle et que la finalité du traitement ne présente pas de risques particuliers (art. 34 al. 3 nLPD).

À noter encore que le Conseil fédéral peut autoriser certains traitements par les organes fédéraux dans le cadre d'essais pilotes (art. 35 nLPD).

C. La proportionnalité

Tout traitement de données personnelles doit être effectué conformément au principe de proportionnalité (art. 6 al. 2 nLPD). Ce principe se divise en trois sous-principes de nécessité, aptitude ou adéquation et proportionnalité au sens étroit[45]. Ainsi le responsable du traitement ne peut traiter que les données qui sont objectivement nécessaires pour atteindre le but poursuivi, qui sont aptes à l'atteindre, et pour autant que le traitement demeure dans un rapport raisonnable entre le résultat légitime recherché et le moyen utilisé, tout en préservant le plus possible le droit des personnes concernées.

En protection des données, on déduit aussi du principe de proportionnalité les principes d'évitement et de minimisation des données. Le premier implique que si le but du traitement peut être atteint sans collecte de données nouvelles, cette option doit être privilégiée[46]. Le second veut que seules les données absolument nécessaires au but poursuivi soient traitées[47].

Le principe de proportionnalité s'applique aux types et aux catégories de données traitées, aux moyens de traitement, aux finalités, à la durée de conservation, etc.[48].

Compte tenu des évolutions technologiques et des capacités presque illimitées de stockage, le Conseil fédéral a estimé qu'il était important de mentionner expressément que les données doivent être détruites ou

---

44 Des exceptions sont envisageables, en particulier si la personne concernée a consenti au traitement en l'espèce, si elle a rendu ses données personnelles accessibles à tout un chacun et ne s'est pas opposée expressément au traitement, ou encore si le traitement est nécessaire pour protéger la vie ou l'intégrité corporelle et qu'il n'est pas possible d'obtenir un consentement dans un délai raisonnable (art. 34 al. 4 nLPD).

45 MEIER, N. 665.

46 MEIER, N. 671-675 ; SHK DSG-BAERISWYL, art. 4 N. 23 ; FF 2017 6644.

47 MEIER, N. 671-675 ; SHK DSG-BAERISWYL, art. 4 N. 23 ; FF 2017 6644.

48 MEIER, N. 676.

anonymisées dès qu'elles ne sont plus nécessaires au regard des finalités du traitement (art. 6 al. 4 nLPD)[49], même si cela découle déjà du principe de proportionnalité, dans son aspect temporel. Pour le Conseil fédéral, il découle de ce principe que le responsable du traitement doit fixer des délais de conservation[50].

D. La finalité

L'art. 6 al. 3 nLPD consacre le principe de finalité ou de respect du but : des données personnelles ne peuvent être collectées que pour des finalités déterminées et reconnaissables pour la personne concernée. Le caractère déterminé des finalités implique que des buts vagues, non définis ou imprécis ne suffisent pas[51]. Cela s'apprécie évidemment selon les circonstances, l'objectif étant principalement de concilier les intérêts des personnes concernées et ceux du responsable du traitement. En cas de communication des données à un tiers, ce dernier est lié par les finalités indiquées au moment de la collecte[52].

La nLPD précise désormais que les données peuvent également être traitées ultérieurement de manière compatible avec les finalités initiales[53]. Le traitement de données liées à l'octroi d'un prêt par une banque pour vérifier spontanément si le client est éligible à un meilleur type de prêt est une finalité compatible avec la finalité initiale, contrairement à la communication des données à un tiers qui souhaite proposer une assurance responsabilité civile au client de la banque.

Cette nouvelle formulation de la nLPD n'implique toutefois pas de changements majeurs puisqu'un traitement ultérieur que la personne concernée considérerait légitimement comme inattendu, inapproprié ou contestable continuerait d'être inadmissible[54]. Lorsque la modification du but initial est prévue par la loi, requise par un changement législatif ou légitimée par un autre motif justificatif, le traitement ultérieur devrait aussi être considéré comme compatible avec le but initial[55].

---

49 FF 2017 6645.

50 FF 2017 6645.

51 MEIER, N. 723 ; FF 2017 6644.

52 MEIER, N. 726.

53 Cela est également connu du RGPD (art. 6 par. 4 RGPD). Voir également ROSENTHAL, N. 35.

54 FF 2017 6644-6645 et les réf. citées.

55 FF 2017 6644-6645 et les réf. citées.

E. La transparence

Le principe de transparence était dans de nombreux cas limité à la reconnaissabilité de l'art. 4 al. 4 aLPD. Il est repris indirectement à l'art. 6 al. 3 nLPD qui prévoit que les données doivent être collectées pour des finalités déterminées et reconnaissables pour la personne concernée. Cette formulation malheureuse n'implique toutefois pas de changements matériels par rapport à l'aLPD tant la collecte des données que les finalités du traitement doivent être reconnaissables[56]. On considère que la reconnaissabilité est remplie lorsqu'on informe la personne concernée, lorsque les traitements sont prévus par la loi ou lorsqu'ils ressortent clairement des circonstances[57].

La portée pratique du principe de transparence est fortement réduite puisque l'art. 19 nLPD a introduit un devoir d'information systématique pour le responsable du traitement privé[58]. La violation du principe de transparence reste une présomption de traitement illicite (art. 30 al. 2 let. a nLPD)[59], mais le non-respect de l'obligation d'information peut désormais être sanctionné par une amende pénale allant jusqu'à 250'000 francs pour les responsables du traitement privés (art. 60 al. 1 let. a nLPD)[60] et par une mesure administrative pour les organes fédéraux (art. 51 al. 3 let. c nLPD).

F. L'exactitude

Celui qui traite des données personnelles doit s'assurer qu'elles sont exactes (art. 6 al. 5 nLPD). Une donnée exacte est une donnée correcte, actuelle et objective[61]. L'obligation d'exactitude n'est pas absolue, mais elle doit être proportionnée à la finalité du traitement. Certaines obligations légales peuvent même s'opposer à la rectification, à l'effacement, ou à la mise à jour des données[62].

Il faut donc prendre toutes les mesures appropriées qui permettent de rectifier, d'effacer ou de détruire les données inexactes ou incomplètes au regard des finalités pour lesquelles elles sont collectées ou traitées. Le caractère approprié des mesures dépend notamment du type de

---

56 FF 2014 6644. Voir également ROSENTHAL, N. 33.

57 FF 2014 6644.

58 Il était précédemment réservé aux données sensibles traitées par les privés et à toutes les données collectées par les organes fédéraux. Voir V. A.

59 Elle peut être justifiée par un motif justificatif de l'art. 31 nLPD.

60 Art. 60 al. 1 nLPD.

61 MEIER, N. 745 ; BSK DSG-LAMBROU / SCHÖNBÄCHLER, art. 5 N. 8.

62 FF 2017 6646 et les réf. citées.

traitement, de son étendue, ainsi que du risque que le traitement des données en question présente pour la personnalité et les droits fondamentaux des personnes concernées (art. 6 al. 5 nLPD). Si des données inexactes ne peuvent pas être rectifiées ou complétées, elles doivent alors être effacées ou détruites[63].

Une donnée inexacte ne doit donc pas être systématiquement détectée et corrigée. Elle doit l'être si elle porte atteinte à la personnalité ou si la personne concernée le demande[64]. Le responsable du traitement n'a pas un devoir de contrôle permanent, mais il doit tenir compte de toutes les modifications dont il a connaissance. Dans le cadre d'une affaire opposant le PFPDT à l'entreprise de renseignements de solvabilité « *Moneyhouse* », le Tribunal administratif fédéral a retenu que si le responsable du traitement doit vérifier que les données qu'il traite sont à jour et que celui qui prétend avoir un intérêt à connaître la solvabilité d'un tiers y est bien légitimé, ces vérifications peuvent avoir lieu par sondage. En l'espèce, il suffisait de vérifier 5 % des données communiquées pour s'assurer qu'elles sont exactes et 3 % des demandes pour s'assurer qu'elles sont justifiées[65].

G. La sécurité

La sécurité des données est mentionnée à l'art. 8 nLPD qui prévoit que les responsables du traitement et les sous-traitants doivent assurer, par des mesures organisationnelles et techniques appropriées, une sécurité adéquate des données personnelles par rapport au risque encouru. Cette disposition matérialise l'approche fondée sur les risques[66]. Plus le risque d'une atteinte à la sécurité des données est élevé, plus les exigences auxquelles doivent répondre les mesures à prendre seront élevées.

Il est encore précisé que les mesures doivent permettre d'éviter toute violation de la sécurité des données, soit toute violation de la sécurité entraînant la perte de données personnelles, leur modification, leur effacement ou leur destruction, leur divulgation ou un accès non autorisés à ces données, et ce indépendamment de la question de savoir si la violation est intentionnelle ou non, licite ou illicite (art. 6 et 8 al. 2 nLPD). Ces mesures peuvent viser par exemple à pseudonymiser des données, à assurer la confidentialité et la disponibilité du système ou de ses

---

63 FF 2017 6646.

64 MEIER, N. 756.

65 TAF A-4232/2015 du 18 avril 2017, c. 7.3.2. Pour un résumé de l'arrêt, voir MÉTILLE / NGUYEN XUAN, Un profil de personnalité n'est pas nécessaire pour juger de la solvabilité d'une personne, *in*: Medialex 2017, pp. 176-179.

66 FF 2017 6650.

services, ou encore à élaborer des procédures visant à tester, à analyser et à évaluer régulièrement l'efficacité des mesures prises[67].

Les exigences minimales en matière de sécurité des données personnelles figureront dans une ordonnance du Conseil fédéral (art. 8 al. 3 nLPD). L'art. 61 let. c nLPD prévoit que les personnes privées qui, intentionnellement, ne respectent pas les exigences minimales en matière de sécurité des données édictées par le Conseil fédéral selon l'art. 8 al. 3 nLPD s'exposent à une amende de 250'000 francs Une plainte est requise.

V. Les obligations du responsable du traitement

A. L'information

Le devoir d'informer lors de la collecte de données personnelles (art. 19 nLPD) vient renforcer le principe de transparence. Il s'applique que les données soient collectées directement auprès de la personne concernée ou d'un tiers (art. 19 al. 1 nLPD). Dans ce dernier cas, le responsable du traitement doit informer la personne concernée au plus tard un mois après avoir obtenu les données, voire au moment de la communication des données s'il les communique avant l'échéance de ce délai d'un mois (art. 19 al. 5 nLPD).

Le devoir d'informer n'est pas absolu et la nLPD prévoit des cas où l'obligation d'informer tombe complètement (art. 20 al. 1 et 2 nLPD) et des cas où le devoir d'informer peut être limité sur la base d'une pesée d'intérêts (art. 20 al. 3 nLPD). Les motifs justificatifs de l'art. 31 nLPD ne sont en revanche pas applicables[68].

Il n'y a ainsi pas de devoir d'informer lorsque la personne concernée a déjà les informations. Cela peut être le cas parce qu'elle avait été informée antérieurement et que les informations n'ont pas changé depuis, ou parce que la personne concernée a déjà reçu les informations en vue de son consentement à un traitement de données. Le Conseil fédéral considère que c'est aussi le cas quand la personne a elle-même communiqué des données sans intervention du responsable du traitement, par exemple lors de la remise d'un dossier de candidature[69]. Si l'on comprend bien que le responsable du traitement ne pouvait pas informer avant de recevoir le dossier, la protection de la bonne foi exige néanmoins qu'il informe sur tous les éléments que la personne concernée ne pouvait pas raisonnablement envisager.

---

67 FF 2017 6650.

68 Dans le même sens, ROSENTHAL, N. 92.

69 FF 2017 6671.

Il n'y a pas non plus d'obligation d'informer lorsque la loi prévoit le traitement des données[70], qu'il soit obligatoire ou envisagé, ou si le responsable du traitement est une personne privée liée par une obligation légale de garder le secret car on estime que l'obligation légale de confidentialité prime sur le devoir d'information[71]. Les médias à caractère périodique bénéficient également, à certaines conditions, d'une exception pour les données traitées exclusivement pour la publication dans la partie rédactionnelle[72].

Il n'y a finalement pas d'obligation d'informer lorsque l'information est impossible à donner ou nécessiterait des efforts disproportionnés et que les données personnelles ne sont pas collectées auprès de la personne concernée. L'information est considérée comme impossible lorsque la personne concernée n'est pas identifiable. Quant aux efforts disproportionnés, ils le sont lorsqu'ils paraissent injustifiés par rapport au bénéfice que la personne concernée retirerait de l'information. Ces exceptions s'appliquent restrictivement[73].

Il n'y a en revanche pas d'exception générale lorsque l'information aurait nécessité des efforts disproportionnés, mais que les données sont collectées directement auprès de la personne concernée. Dans ce cas, il faudrait procéder à une pesée d'intérêts au sens de l'art. 20 al. 3 nLPD.

La limitation de l'information prévue par l'art. 20 al. 3 nLPD prévoit une pesée d'intérêt et permet, selon les cas de renoncer, restreindre ou différer l'information. La liste des cas de limitation est exhaustive et la disposition doit être interprétée restrictivement[74]. Le principe de proportionnalité s'applique et l'on choisira, de manière générale, la solution la plus favorable à la personne concernée, garantissant la transparence maximale du traitement compte tenu des circonstances[75].

Le premier cas de limitation est justifié par les intérêts prépondérants d'un tiers. Le deuxième cas vise des situations particulières où le fait d'informer la personne concernée empêche totalement le traitement d'atteindre son but principal. Il ne suffit pas que l'absence d'information soit plus pratique pour le responsable du traitement ou qu'elle soit justifiée par des intérêts purement économiques[76]. Le troisième cas

---

70 Ce qui revient à dire que l'obligation d'informer des organes fédéraux est très limitée (dans le même sens : ROSENTHAL, N. 103).

71 FF 2017 6671.

72 Dans le cas où l'information fournirait des indications sur les sources d'information, qu'il en résulterait un droit de regard sur des projets de publication ou que la libre formation de l'opinion publique serait compromise (art. 27 nLPD).

73 FF 2017 6671.

74 FF 2017 6672.

75 FF 2017 6672.

76 FF 2017 6673. Sur la forme de l'information, voir notamment ROSENTHAL, N. 99.

prend en compte les intérêts prépondérants du responsable du traitement privé[77] à la condition qu'il ne communique pas les données à des tiers (responsables du traitement). La communication de données entre des entreprises contrôlées par une même personne morale n'est pas considérée comme une communication à des tiers en application de cette disposition (art. 18 al. 4 nLPD)[78].

La loi ne précise pas la manière de fournir l'information, mais la personne concernée doit l'obtenir sans avoir à la demander. L'information doit être facilement accessible, mais le responsable du traitement ne doit pas s'assurer que la personne concernée en a effectivement pris connaissance. Une information générale sous forme de conditions générales, de déclaration de confidentialité sur un site web ou des pictogrammes[79] est admissible si elle contient tous les éléments nécessaires[80].

Le responsable du traitement doit donc communiquer à la personne concernée toutes les informations nécessaires pour qu'elle puisse faire valoir ses droits selon la nLPD et pour garantir la transparence des traitements. L'art. 19 al. 2 nLPD dresse la liste des informations minimales à communiquer, soit l'identité et les coordonnées du responsable du traitement, la finalité du traitement, les destinataires ou les catégories de destinataires[81] si les données personnelles leur sont transmises, les pays ou organismes internationaux concernés et les garanties prévues[82] s'il y a un transfert à l'étranger, ainsi que les catégories de données traitées si les données personnelles ne sont pas collectées auprès de la personne concernée.

Contrairement à ce qui est prévu en droit européen, il n'y a pas d'obligation d'indiquer les droits de la personne concernée ou la durée de conservation des données.

Si la violation du principe de transparence reste une présomption de traitement illicite (art. 30 al. 2 let. a nLPD)[83], le non-respect de

---

77 Lorsque le responsable du traitement est un organe fédéral, l'exception s'applique s'il y a un intérêt public prépondérant, en particulier la sûreté intérieure ou extérieure de la Suisse, ou si la communication des informations est susceptible de compromettre une enquête, une instruction ou une procédure judiciaire ou administrative (art. 20 al. 3 let. d nLPD).

78 Art. 20 al. 4 nLPD.

79 Voir par exemple les Privacy Icons: THOUVENIN / GLATTHAAR / HOTZ / ETTLINGER / TSCHUDIN, N. 1 ss.

80 FF 2017 6668.

81 Cela inclut tant les sous-traitants que les tiers.

82 Des garanties sont nécessaires en cas de transfert vers un pays qui n'est pas considéré comme adéquat au sens de l'art. 16 al. 1 nLPD. Si le transfert est justifié par une dérogation de l'art. 17 nLPD, elle doit aussi être indiquée.

83 Elle peut être justifiée par un motif justificatif de l'art. 31 nLPD.

l'obligation d'information peut désormais être sanctionné par une amende pénale allant jusqu'à 250'000 francs pour les responsables du traitement privés[84] et par une mesure administrative pour les organes fédéraux[85].

B. Le registre des activités de traitement

L'obligation prévue par l'art. 11a aLPD de déclarer certains fichiers a été remplacée par une obligation de tenir un registre des activités de traitement (art 12 nLPD)[86]. Cette obligation s'applique à tous les responsables du traitement et les sous-traitants qui emploient au moins 250 collaborateurs (art. 12 al. 1 et 5 nLPD). Pour les personnes individuelles et les entreprises de moins de 250 collaborateurs, le Conseil fédéral peut prévoir des exceptions dans l'ordonnance pour alléger leur charge, à la condition que le traitement ne représente qu'un risque limité[87]. Le PFPDT peut avoir accès au registre des responsables du traitement privés sur demande, mais pas les personnes concernées. En revanche, le registre des organes fédéraux est publiquement accessible (art. 56 nLPD).

Le registre n'est ni une copie des données personnelles traitées, ni un journal détaillé des traitements. C'est un descriptif général des activités de traitement qui permet d'avoir une vue d'ensemble de tous les traitements et de se faire rapidement une idée sur la conformité des traitements. Son contenu correspond dans une large mesure aux indications que la personne concernée doit recevoir en vertu du devoir d'information et du droit d'accès.

L'art. 12 al. 2 nLPD précise les indications minimales que doit contenir le registre du responsable du traitement : l'identité (le nom) du responsable du traitement (let. a), la finalité du traitement (let. b), une description des catégories des personnes concernées et des catégories de données personnelles traitées (let. c), les catégories des destinataires auxquels les données sont susceptibles d'être communiquées (let. d), le délai de conservation des données personnelles ou les critères selon lesquels ce délai est fixé (let. e), si possible une description générale des mesures de sécurité (let. f), et en cas de communication à l'étranger,

---

84 Art. 60 al. 1 nLPD.

85 Art. 51 al. 3 nLPD.

86 Un tel registre est également prévu par l'art. 30 RGPD.

87 FF 2017 6656.

le nom de l'État en question[88] et les garanties prises selon l'art.13 al. 2 nLPD (let. g). Il n'y a pas d'exigence de forme[89].

Le registre du sous-traitant doit contenir l'identité du sous-traitant et du responsable du traitement, les catégories de traitements effectués pour le compte du responsable du traitement, si possible une description générale des mesures de sécurité, et en cas de communication à l'étranger, le nom de l'État en question et les garanties prises selon l'art. 21 al. 2 nLPD[90].

Le nom du responsable du traitement et la finalité n'appellent pas de commentaires particuliers. Les catégories des personnes concernées s'entendent comme des groupes partageant les mêmes caractéristiques[91]. Il en va de même pour les catégories des destinataires[92]. Quant aux catégories des données traitées, elles doivent permettre de savoir quel type de données sont traitées sans que la donnée elle-même ne doive être indiquée[93].

La description générale des mesures visant à garantir la sécurité des données devrait faire apparaître d'éventuels manquements dans les mesures de sécurité. Elle n'est obligatoire que si les mesures peuvent être définies de manière suffisamment concrète[94].

C. Le représentant

Le responsable du traitement privé qui a son siège ou son domicile à l'étranger et traite des données personnelles concernant des personnes en Suisse doit désigner un représentant en Suisse lorsque l'une des cinq conditions suivantes est remplie (art. 14 al. 1 nLPD) : le traitement est en rapport avec une offre de biens ou de services en Suisse (let. a), le traitement est en rapport avec un suivi du comportement de ces personnes en Suisse (let. a), il s'agit d'un traitement de données personnelles à grande échelle (let. b), il s'agit d'un traitement régulier de données personnelles (let. c), ou le traitement présente un risque élevé pour la personnalité des personnes concernées (let. d). Cette obligation a été introduite par le Parlement.

---

88 Cette exigence, qui n'est pas connue du RGPD, sera extrêmement difficile à respecter en pratique.

89 Dans le même sens : ROSENTHAL, N. 145.

90 Art. 6 al. 2 let. f nLPD.

91 Par exemple des clients, des employés, des abonnés, des concurrents, etc.

92 Par exemple des sous-traitants, des autorités de surveillance, des entreprises appartenant au même groupe, etc.

93 Par exemple le nom, le prénom, l'adresse, la langue de correspondance, les données relatives aux achats, les préférences publicitaires, etc.

94 FF 2017 6655.

Le responsable du traitement doit évidemment publier le nom et l'adresse de son représentant (art. 14 al. 3 nLPD), mais un enregistrement auprès du PFPDT n'est étonnamment pas prévu par la loi. Il sert de point de contact pour les personnes concernées et le PFPDT (art. 14 al. 2 nLPD). Conformément à l'art. 15 al. 1 nLPD, le représentant doit en particulier tenir un registre des activités de traitement du responsable du traitement qui contient les indications mentionnées à l'art. 12 al. 2 nLPD, fournir sur demande au PFPDT les indications contenues dans ce registre (art. 15 al. 2 nLPD) et fournir sur demande à la personne concernée des renseignements concernant l'exercice de ses droits (art. 15 al. 3 nLPD)[95].

D. Le conseiller à la protection des données.

Le conseiller à la protection des données figure désormais dans la loi, mais de manière limitée. L'art.10 nLPD constate simplement que les responsables du traitement privés peuvent nommer un conseiller à la protection des données. Il s'agit toujours d'une faculté et en aucun cas d'une obligation[96]. C'est en revanche une obligation pour les organes fédéraux, comme précédemment (art. 10 al. 4 nLPD)[97].

Si le responsable du traitement choisit de nommer un conseiller, le législateur a jugé utile de préciser qu'il sera alors l'interlocuteur des personnes concernées et des autorités chargées de la protection des données en Suisse (art. 10 al. 2 nLPD). Il aura notamment pour tâches de former et conseiller le responsable du traitement en matière de protection des données (art. 10 al. 2 let. a nLPD), ainsi que de concourir à l'application des prescriptions relatives à la protection des données (art. 10 al. 2 let. b nLPD).

Le seul bénéfice légal de la désignation d'un conseiller est que le responsable du traitement peut renoncer à consulter le PFPDT lorsque l'analyse d'impact relative a révélé que le traitement présente encore un risque élevé malgré les mesures prévues par le responsable du traitement pour atténuer ce risque, à la condition d'avoir consulté son conseiller (10 al. 3 et art. 23 al. 4 nLPD).

Pour bénéficier de cet allégement (art. 10 al. 3 nLPD), il faut que le conseiller exerce sa fonction de manière indépendante par rapport au responsable du traitement et sans recevoir d'instruction de celui-ci (let. a), qu'il n'exerce pas de tâches incompatibles avec ses tâches de

---

95 Cela vise seulement une information générale sur les droits de la personne concernée, par opposition à l'art. 19 nLPD qui vise l'accès aux données nécessaires pour qu'elle puisse faire valoir ses droits.

96 FF 2017 6652.

97 Cette obligation sera reprise dans l'ordonnance (FF 2017 6653).

conseiller (let. b), qu'il dispose des connaissances professionnelles nécessaires (let. c), et que le responsable du traitement ait publié les coordonnées du conseiller et les ait communiquées au PFPDT (let. d).

Le conseiller peut être interne ou externe. Si c'est un collaborateur, son indépendance doit être garantie par la hiérarchie en place dans l'entreprise en le subordonnant en principe directement à la direction du responsable du traitement. L'interdiction d'exercer des tâches incompatibles empêchera en principe qu'il soit membre de la direction, qu'il exerce des fonctions dans les domaines de la conduite du personnel ou de la gestion des systèmes informatiques, ou qu'il appartienne à un service qui traite des données personnelles sensibles. Les fonctions de conseiller à la protection des données et de délégué à la sécurité de l'information ne semblent en revanche pas incompatibles pour le Conseil fédéral[98].

E. La sous-traitance

Le responsable du traitement peut recourir à des sous-traitants pour effectuer certaines opérations. Les traitements au sein d'une même personne juridique (succursale, unité administrative, employé) ne constituent en principe pas des cas de sous-traitance)[99].

L'art. 9 nLPD reprend en substance les mêmes conditions que celles de l'ancien droit, à savoir que le responsable du traitement peut confier le traitement de données personnelles à un sous-traitant si la loi ou un contrat le prévoit (art. 9 al. 1 let. a nLPD). Le sous-traitant ne peut effectuer que les traitements que le responsable du traitement est en droit d'effectuer lui-même et toute obligation légale ou contractuelle de garder le secret doit être respectée (art. 9 al. 1 let. b nLPD). Le consentement de la personne concernée n'est pas nécessaire[100], mais la personne concernée doit être informée de l'existence de destinataires (ou catégories de destinataires), parmi lesquels figurent les sous-traitants (art. 19 al. 2 let. c nLPD).

Contrairement au RGPD, il n'y a aucune exigence sur le contenu du contrat, ni sur sa forme qui peut continuer à être orale. On préférera évidemment pour des raisons de preuve un contrat écrit.

L'art. 9 al. 3 nLPD est nouveau et prévoit une interdiction pour le sous-traitant de sous-traiter à son tour (délégation de deuxième rang) sans avoir l'autorisation préalable du responsable du traitement. L'autorisation peut être spécifique ou générale. Si l'autorisation est générale,

---

98 FF 2017 6652-6653.

99 FF 2017 6652.

100 Dans le même sens : ROSENTHAL, N. 57.

le responsable du traitement devrait prévoir que le sous-traitant l'informe préalablement de tout changement (ajout ou remplacement d'autres sous-traitants). Dans le secteur privé, l'autorisation n'est soumise à aucune exigence de forme[101].

Comme dans le droit actuel, la sous-traitance des données personnelles qui sont protégées par un secret n'est pas exclue, mais les conditions particulières applicables au secret concerné doivent être respectées. Par exemple dans le cas du secret professionnel, pour que la sous-traitance soit possible, le sous-traitant devra pouvoir être qualifié d'auxiliaire au sens de l'art. 321 CP[102].

Le responsable du traitement a donc un devoir de diligence dans le but de sauvegarder les droits des personnes concernées. Il doit s'assurer de manière active que le sous-traitant respecte la loi dans la même mesure que lui. Cela concerne non seulement les règles relatives à la sécurité, mais aussi le respect des principes généraux de protection des données. Par analogie avec l'art. 55 CO, il doit mettre tout en œuvre pour éviter d'éventuelles violations de la nLPD. Il doit ainsi veiller à choisir soigneusement son mandataire (*curia in eligendo*), à lui donner les instructions adéquates (*curia in instruendo*) et à exercer la surveillance nécessaire (*curia in custodiendo*)[103].

Le fait de confier intentionnellement le traitement de données personnelles à un sous-traitant sans respecter les conditions de l'art. 9 al. 1 et 2 nLPD est une contravention sanctionnée par une amende pénale allant jusqu'à 250'000 francs pour les responsables du traitement privés (art. 61 let. b nLPD).

F. Le transfert à l'étranger

Le principe de l'ancien droit selon lequel aucune donnée personnelle ne pouvait être transmise à l'étranger si la personnalité des personnes concernées devait s'en trouver gravement menacée a été supprimé, car il créait trop d'insécurités juridiques[104].

Le principe est désormais que des données personnelles peuvent être communiquées à l'étranger si le Conseil fédéral a constaté que l'État concerné dispose d'une législation assurant un niveau de protection adéquat[105]. Le Conseil fédéral publiera la liste des États assurant un niveau de protection adéquat sous la forme d'une ordonnance publiée

---

101 FF 2017 6651.

102 FF 2017 6651.

103 MEIER, N. 1218.

104 FF 2017 6657.

105 Art. 16 al. 1 nLPD. Voir également ROSENTHAL, N. 64 ss.

au Recueil officiel[106]. Dès qu'un État figure dans la liste, la libre circulation des données personnelles de la Suisse vers cet État est garantie, sans autre mesure de vérification du responsable du traitement[107]. Dans le cadre de cet examen, il appartiendra au Conseil fédéral d'examiner si l'État étranger dispose tout d'abord d'une législation remplissant les standards de la Convention 108 modernisée et, d'autre part, d'examiner comment cette législation est mise en œuvre[108].

En l'absence d'une décision du Conseil fédéral, des données personnelles peuvent être communiquées à l'étranger si un niveau de protection approprié est garanti par d'autres moyens (art. 16 al. 2 nLPD)[109] ou si une dérogation s'applique (art. 17 nLPD)[110]. Un niveau de protection adéquat peut en particulier être garanti par un traité international (art. 16 al. 2 let. a nLPD) ou des clauses contractuelles (clauses contractuelles[111] entre l'exportateur des données et le destinataire à l'étranger ou des règles d'entreprise contraignantes[112]). On soulignera toutefois que les garanties contractuelles ne peuvent pas déroger au droit impératif de l'État de destination, et que dans certains cas aucun engagement contractuel ne pourra garantir un niveau de protection suffisant[113].

Les dérogations (art. 17 nLPD) concernent des situations particulières. C'est en particulier le cas lorsque la personne concernée a expressément donné son consentement à la communication, après avoir été informée de l'État en question et des risques du transfert dans cet État, ou si la communication est en relation directe avec la conclusion ou l'exécution d'un contrat, non seulement entre le responsable du traitement et la personne concernée, mais aussi entre le responsable du

---

106 FF 2017 6657.

107 FF 2017 6657-6658.

108 FF 2017 6657.

109 ROSENTHAL, N. 71 ss.

110 ROSENTHAL, N. 75 ss.

111 Des clauses types de protection des données préalablement approuvées par le PFPDT (art. 16 al. 2 let. d nLPD), un contrat entre le responsable du traitement (ou le sous-traitant) et son cocontractant à l'étranger préalablement communiquées au PFPDT (art. 16 al. 2 let. b nLPD), ou des garanties spécifiques élaborées par l'organe fédéral et préalablement communiquées au PFPDT (art. 16 al. 2 let. c nLPD). Le RGPD prévoit un système similaire. Voir à ce propos COMITÉ EUROPÉEN DE LA PROTECTION DES DONNÉES, Guidelines 2/2020 on articles 46 (2) (a) and 46 (3) (b) of Regulation 2016/679 for transfers of personal data between EEA and non-EEA public authorities and bodies du 15 décembre 2020.

112 Des règles d'entreprise contraignantes préalablement approuvées par le PFPDT ou son homologue dans un État assurant un niveau de protection adéquat (art. 16 al. 2 let. e nLPD).

113 Voir notamment arrêt CJUE Maximilian Schrems et Data Protection Commissionner contre Facebook Ireland Ltd, C-311/18 du 16 juillet 2020.

traitement et son cocontractant, dans l'intérêt de la personne concernée (art. 17 al. 1 let. a et b nLPD)[114].

C'est également le cas lorsque la communication est nécessaire à la sauvegarde d'un intérêt public prépondérant, à la constatation, à l'exercice ou à la défense d'un droit devant un tribunal ou une autre autorité étrangère (art. 17 al. 2 let. c nLPD), ou pour protéger la vie ou l'intégrité corporelle de la personne concernée ou d'un tiers (art. 17 al. 2 let. d nLPD)[115]. C'est finalement aussi le cas si la personne concernée a rendu les données personnelles accessibles à tout un chacun et ne s'est pas opposée expressément au traitement (art. 17 al. 2 let. e nLPD) ou si les données proviennent d'un registre prévu par la loi et destiné à fournir des informations au public (art. 17 al. 2 let. f nLPD)[116].

Le PFPDT peut suspendre ou interdire la communication de données personnelles à l'étranger si elle est contraire aux conditions des art. 16 ou 17 nLPD ou à des dispositions d'autres lois fédérales concernant la communication de données personnelles à l'étranger (art. 51 al. 2 nLPD).

Le fait de communiquer intentionnellement des données personnelles à l'étranger en violation de l'art. 16 al. 1 et 2 nLPD (sans que les conditions de l'art. 17 nLPD ne soient remplies) est une contravention sanctionnée par une amende pénale allant jusqu'à 250'000 francs pour les responsables du traitement privés (art. 61 let. a nLPD).

G. L'analyse d'impact relative à la protection des données personnelles

La nLPD introduit l'analyse d'impact relative à la protection des données (art. 22 nLPD)[117]. Il s'agit d'un outil préventif à destination du responsable du traitement qui devrait lui permettre, après avoir décrit le traitement qu'il entend mettre en œuvre, d'en évaluer la nécessité et la proportionnalité tout en évaluant les risques pesant sur les droits et libertés des personnes physiques au vu du traitement envisagé. En cas

---

114 FF 2017 6661.

115 Seulement s'il n'est pas possible d'obtenir le consentement de la personne concernée dans un délai raisonnable.

116 Seulement s'il est accessible au public ou à toute personne justifiant d'un intérêt légitime et pour autant que les conditions légales pour la consultation dans le cas d'espèce soient remplies.

117 Cette obligation est également connue du droit européen (art. 35 RGPD). Voir également COMITÉ EUROPÉEN DE LA PROTECTION DES DONNÉES, Recommandation 01/2019 sur le projet de liste établi par le Contrôleur européen de la protection des données concernant les opérations de traitement pour lesquelles une analyse d'impact relative à la protection des données est requise (art. 39 par. 4 du règlement (UE) 2018/1725) du 10 juillet 2019 et GROUPE DE TRAVAIL « ARTICLE 29 », 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 du 4 octobre 2017.

de risque, le responsable du traitement doit déterminer les mesures nécessaires pour y faire face[118].

Une analyse d'impact n'est requise que lorsque le traitement envisagé est susceptible d'entraîner un risque élevé pour la personnalité ou les droits fondamentaux de la personne concernée et doit être réalisée préalablement à ce traitement (art. 22 al. 1 nLPD). Elle n'est pas nécessaire si le traitement repose sur une obligation légale (art. 22 al. 4 nLPD). Le responsable du traitement peut également renoncer à établir une analyse d'impact dans certaines hypothèses (art. 22 al. 5 nLPD). C'est notamment le cas lorsqu'il recourt à un système, un produit ou un service certifié conformément à l'art. 13 nLPD ou s'il respecte un code de conduite au sens de l'art. 11 nLPD, faut-il encore que celui-ci repose sur une analyse d'impact (art. 22 al. 5 let. a), qu'il prévoie des mesures pour protéger la personnalité et les droits fondamentaux de la personne concernée (art. 22 al. 5 let. b nLPD) et qu'il ait été soumis au PFPDT (art. 22 al. 5 let. c nLPD).

Sous réserve de ces exceptions, le responsable du traitement doit réaliser une analyse d'impact lorsque le traitement est susceptible d'entraîner un risque élevé. La notion de risque élevé est complexe et floue[119]. Le risque dépend notamment de la nature, de l'étendue, des circonstances, de la finalité du traitement et du type de technologies utilisées. De manière logique, il y a lieu de conclure à un risque élevé selon si le traitement est étendu, selon le caractère sensible des données ou encore si la finalité du traitement est vaste[120]. L'art. 22 al. 2 nLPD souligne qu'un risque élevé existe notamment dans deux cas, le premier étant si le responsable du traitement traite des données sensibles à grande échelle (let. a) et le second étant lorsque le responsable du traitement opère une surveillance systématique de grandes parties du domaine public (let. b). Cette liste n'est pas exhaustive et il appartient au responsable du traitement d'évaluer l'opportunité de réaliser une telle analyse d'impact, préalablement à tout traitement. Bien qu'il s'agisse d'une obligation, sa violation n'est pas sanctionnée pénalement. Le PFPDT peut toutefois ordonner à la personne privée ou à l'organe fédéral dans le cadre d'une enquête d'en établir une (art. 51 al. 3 let. d nLPD).

L'art. 22 al. 3 nLPD prévoit ce que doit contenir une analyse d'impact, à savoir une description du traitement envisagé, une évaluation des risques pour la personnalité ou les droits fondamentaux de la personne concernée, ainsi que les mesures prévues pour protéger sa personnalité et ses droits fondamentaux. Autrement dit, l'analyse d'impact doit

---

118 DI TRIA, p. 119 ; FF 2017 6676.

119 Sur l'évaluation de la notion de risque élevé dans le cadre d'une analyse d'impact, cf. DI TRIA, pp. 123 ss.

120 FF 2017 6676.

contenir une étude du contexte et des enjeux du traitement envisagé, des mesures prévues, des risques liés à la sécurité des données, de leur impact sur la vie privée ainsi qu'une phase de validation et de suivi. Il s'agit en somme d'un inventaire des risques et des mesures potentiellement applicables[121]. Si la nLPD ne contient pas de méthodologie à adopter pour réaliser une analyse d'impact, il est possible de s'inspirer de ce qui est conseillé par les autorités de contrôle européennes. Ces dernières ont développé un processus en sept étapes, qui commence par la description des opérations de traitement envisagées, l'évaluation de la nécessité et de la proportionnalité du traitement, les mesures envisagées pour démontrer la conformité, l'évaluation des risques pour les droits et libertés, les mesures envisagées pour faire face aux risques. Les deux dernières étapes consistent à documenter le processus et d'en assurer un suivi[122].

H. L'annonce des violations de la sécurité des données

La violation de la sécurité des données est définie comme toute violation de la sécurité entraînant de manière accidentelle ou illicite la perte de données personnelles, leur modification, leur effacement ou leur destruction, leur divulgation ou un accès non autorisés à ces données (art. 5 let. h nLPD). La violation peut être causée par un tiers, mais son auteur peut aussi être un collaborateur qui outrepasse ses compétences ou qui fait preuve de négligence. La violation de la sécurité des données peut entraîner une perte de contrôle de la personne concernée sur ses données ou une utilisation abusive de celles-ci. Elle peut aussi engendrer une violation de la personnalité, par exemple en entraînant la divulgation d'informations que la personne souhaitait garder secrètes[123].

Si la violation de la sécurité des données entraîne vraisemblablement un risque élevé[124] pour la personnalité ou les droits fondamentaux de la personne concernée, le responsable du traitement doit l'annoncer dans les meilleurs délais au PFPDT (art. 24 al. 1 nLPD)[125]. Plus le risque est élevé et le nombre de personnes concernées important, plus l'annonce

---

121 DI TRIA, p. 129.

122 DI TRIA, p. 130 ; FF 2017 6678.

123 FF 2017 6680-6681.

124 La notion de risque élevé est propre à l'annonce de la violation de sécurité et ne correspond pas forcément celle du risque élevé en matière d'analyse d'impact. Dans le même sens, ROSENTHAL, N. 163.

125 Une obligation similaire est prévue aux art. 33 et 34 RGPD. Voir notamment GROUPE DE TRAVAIL « ARTICLE 29 », Lignes directrices sur la notification de violations de données à caractère personnel en vertu du RGPD du 3 octobre 2017 ainsi COMITÉ EUROPÉEN DE LA PROTECTION DES DONNÉES, Guidelines 01/2021 on Examples regarding Data Breach Notification du 19 janvier 2021.

doit intervenir rapidement[126]. De plus, à la demande du PFPDT ou si cela est nécessaire à la protection de la personne concernée, le responsable du traitement doit également informée cette dernière (art. 24 al. 4 nLPD). L'information à la personne concernée devrait toujours intervenir lorsque cela lui permet de réduire les risques en prenant des dispositions pour se protéger, comme la modification de mots de passe.

L'annonce doit indiquer au minimum la nature de la violation (effacement ou destruction de données, leur perte, leur modification ou leur communication à des tiers non autorisés), les conséquences pour la personne concernée et les mesures prises ou envisagées pour remédier à la situation ou pour atténuer ses conséquences (art. 24 al. 2 nLPD)[127].

Si la violation de la sécurité des données s'est produite chez le sous-traitant, il ne doit pas l'annoncer au PFPDT, mais informer dans les meilleurs délais le responsable du traitement (art. 24 al. 3 nLPD). L'annonce est ici due pour toute violation, sans qu'il soit nécessaire qu'elle entraîne un risque élevé.

Le responsable du traitement peut restreindre l'information à la personne concernée, la différer ou y renoncer dans certains cas (art. 24 al. 5 nLPD), mais pas l'information au PFPDT. C'est en particulier le cas si les intérêts prépondérants d'un tiers l'exigent, si un devoir légal de garder le secret l'interdit, ou si le devoir d'informer est impossible à respecter ou nécessite des efforts disproportionnés. On considère que le devoir d'informer est réputé impossible à respecter lorsque le responsable du traitement n'est pas en mesure d'identifier les personnes concernées par la violation de la sécurité des données. On estime que l'information nécessite des efforts disproportionnés dès lors qu'il faudrait informer individuellement un grand nombre de personnes concernées et que les coûts qui en résulteraient semblent excessifs au regard du gain qu'en retireraient les personnes concernées[128].

Le responsable du traitement peut aussi choisir d'informer la personne concernée par une communication publique, à la condition que l'information des personnes concernées soit garantie de manière équivalente. On estime que cette condition est remplie quand une annonce individuelle ne permettrait pas d'améliorer sensiblement l'information de la personne concernée[129].

---

126 FF 2017 6681.

127 FF 2017 6681.

128 FF 2017 6682.

129 FF 2017 6682.

I. Le profilage à risque élevé

La nLPD a introduit les notions de profilage (art. 5 let. f nLPD) et de profilage à risque élevé (art. 5 let. g nLPD)[130]. Le profilage recouvre toute forme de traitement automatisé de données personnelles consistant à utiliser ces données pour évaluer certains aspects personnels relatifs à une personne physique, notamment pour analyser ou prédire des éléments concernant le rendement au travail, la situation économique, la santé, les préférences personnelles, les intérêts, la fiabilité, le comportement, la localisation ou les déplacements de cette personne physique. Cette définition correspond à celle du RGPD[131]. En quelque sorte, le profilage débute là où s'arrêtait le profil de personnalité[132]: il faut un traitement automatisé et un but d'évaluation. Quant au profilage à risque élevé, c'est celui qui entraîne un risque élevé pour la personnalité ou les droits fondamentaux de la personne concernée, parce qu'il conduit à un appariement de données qui permet d'apprécier les caractéristiques essentielles de la personnalité d'une personne physique. La différence entre profilage et profilage à risque élevé a beaucoup agité l'Assemblée fédérale et le public, mais sa portée est limitée[133]. En pratique, les obligations particulières déclenchées par le profilage concernent surtout l'administration fédérale, alors qu'il faut un profilage à risque élevé pour que les responsables du traitement privés soient concernés.

Ainsi, si un consentement est requis, le consentement doit être exprès lorsqu'il s'agit d'un profilage à risque élevé effectué par une personne privée (art. 6 al. 7 let. b nLPD) ou un organe fédéral, mais également s'il s'agit d'un simple profilage effectué par un organe fédéral (art. 6 al. 7 let. c nLPD). Cela n'implique toutefois pas qu'un consentement est obligatoire que ce soit pour un profilage ou un profilage à risque élevé. La base légale doit de plus être formelle (et pas seulement matérielle) pour qu'un organe fédéral puisse faire un profilage à risque élevé (art. 34 al. 2 let. b nLPD).

Finalement, le profilage à risque élevé n'est pas permis dans le but d'évaluer la solvabilité de la personne concernée, ou plus justement dit

---

130 La notion de profilage à haut risque ne figurait pas dans le P-LPD et a été introduite par le Conseil des États. Ce n'est qu'en séance de conciliation que les chambres ont réussi à se mettre d'accord sur cette notion.

131 Art. 4 ch. 4 RGPD.

132 ROSENTHAL, N. 24.

133 ROSENTHAL, N. 28.

le responsable du traitement privé ne peut pas faire valoir un intérêt prépondérant à effectuer un profilage à risque élevé dans ce but[134].

J. La décision individuelle automatisée

L'art. 21 nLPD prévoit une obligation particulière d'informer et d'entendre la personne concernée en cas de décision individuelle automatisée qui a des effets juridiques sur la personne concernée ou qui l'affecte de manière significative.

Par décision individuelle automatisée, il faut entendre une décision prise exclusivement sur la base d'un traitement de données personnelles automatisé sans qu'une décision ne soit prise par une personne physique sur la base de sa propre évaluation de la situation. Les décisions simples du genre de celles qui sont prises lors d'un retrait au bancomat (délivrance du montant demandé si le solde en compte est suffisant) ne sont pas concernées. Le fait que la décision soit communiquée par une personne physique ne change rien à son caractère automatisé, car cette personne n'a pas d'influence sur le processus de décision[135].

Ces obligations ne s'appliquent que si la décision a pour la personne concernée des effets juridiques[136] ou l'affecte de manière significative[137]. En revanche, ces obligations ne s'appliquent pas lorsque la décision est en relation directe avec la conclusion ou l'exécution d'un contrat entre le responsable du traitement et la personne concernée et que la demande de cette dernière est satisfaite (art. 21 al. 3 let. a nLPD), ou encore si la personne concernée a expressément consenti à ce que la décision soit prise de manière automatisée (art. 21 al. 3 let. b nLPD). Dans le premier cas, on suppose que l'information n'intéresse plus la personne concernée, alors que dans le second elle a déjà reçu l'information avant de donner un consentement juridiquement valable[138].

Le responsable du traitement doit donner à la personne concernée qui le demande, la possibilité de faire valoir son point de vue sur le résultat de la décision, et même de demander comment la décision a été prise.

---

134 Une autre justification est en revanche envisageable, en particulier le consentement de la personne concernée.

135 FF 2017 6674.

136 Par exemple, la conclusion ou la dénonciation d'un contrat. Voir également ROSENTHAL, N. 109.

137 Par exemple, la personne concernée est entravée sur le plan économique ou personnel. Il est nécessaire de prendre en compte l'importance du bien en question, la durée des effets de la décision et l'existence ou non d'une solution de remplacement (FF 2017 6674).

138 FF 2017 6675.

Le but est entre autres d'éviter que le traitement de données soit effectué sur la base de données incomplètes, dépassées ou non pertinentes[139].

K. La protection des données dès la conception

La révision de la nLPD a introduit l'obligation de mettre en place, dès la conception du traitement, des mesures techniques et organisationnelles afin de garantir le respect des prescriptions en matière de protection des données et en particulier les principes fixés à l'art. 6 nLPD (art. 7 al. 1 et 2 nLPD)[140]. Il ne s'agit pas d'un principe à proprement parler dont la violation constituerait une atteinte à la personnalité au sens de l'art. 30 al. 2 nLPD.

La protection des données dès la conception repose sur l'idée que la technologie doit être au service de la protection des données personnelles et que la majorité des violations de la sphère privée ne sont pas détectées[141]. Il faut donc éviter qu'elles ne se produisent plutôt que chercher à les sanctionner. Ce concept, initialement développé par *Ann Cavoukian* puis adopté lors de la 32e Conférence internationale des autorités de protection des données[142], repose sur sept principes fondamentaux : prendre des mesures proactives et non réactives, des mesures préventives et non correctives ; assurer la protection implicite de la vie privée, intégrer la protection de la vie privée dans la conception des systèmes et des pratiques, assurer une fonctionnalité complète selon un paradigme à somme positive et non à somme nulle ; assurer la sécurité de bout en bout, pendant toute la période de conservation des renseignements ; assurer la visibilité et la transparence ; et respecter la vie privée des utilisateurs[143].

La protection technique des données personnelles ne s'appuie pas sur une technologie spécifique, mais elle passe plutôt par la mise en place d'un ensemble de règles techniques et organisationnelles intégrées dans le système, de manière à rendre impossible, ou peu probable, une violation de la protection des données[144].

---

139 FF 2017 6675.

140 Cette obligation figure également à l'art. 25 par. 1 RGPD. Voir notamment COMITÉ EUROPÉEN DE LA PROTECTION DES DONNÉES, Guidelines 4/2019 on Article 25 Data Protection by Design and by Default, Version 2.0 du 20 octobre 2020 ; HARTUNG, *in* : Kühling / Buchner, art. 25 N. 1 ss ; BYGRAVE, *in* : Kuner / Bygrave / Docksey, art. 25 N. 1 ss.

141 FF 2017 6648.

142 Voir à cet égard la résolution en lien avec la protection des données dès la conception à l'adresse suivante : < https://edps.europa.eu/sites/edp/files/publication/10-10-27_jerusalem_resolutionon_privacybydesign_en.pdf> (consulté le 01.02.2021).

143 CAVOUKIAN, pp. 1 ss.

144 FF 2017 6648-6649.

La protection des données dès la conception matérialise le principe de proportionnalité et l'approche fondée sur les risques. Il faut établir un rapport entre le risque induit par le traitement et les moyens techniques permettant de le réduire. Plus le risque est élevé, plus sa survenue est probable, et plus le traitement de données est important, plus les exigences auxquelles doivent répondre les mesures techniques pour être considérées comme appropriées au sens de cette disposition seront élevées[145].

Les mesures techniques et organisationnelles doivent ainsi être appropriées au regard notamment de l'état de la technique, du type de traitement, de son étendue, ainsi que du risque que le traitement des données en question présente pour la personne concernée (art. 6 al. 2 nLPD).

L. La protection des données par défaut

La révision de la nLPD a également introduit l'obligation pour le responsable du traitement de garantir, par le biais de préréglages appropriés, que le traitement de données est limité au minimum requis par la finalité poursuivie, à moins que la personne concernée n'en dispose autrement (art. 7 al. 3 nLPD)[146].

Ainsi sans action spécifique de la personne concernée, elle bénéficie du régime le plus respectueux possible de sa personnalité. Elle ne devrait par exemple pas être obligée de créer un compte client pour effectuer une commande en ligne. Ce n'est que si elle choisit de modifier les paramètres prédéfinis qu'elle opte pour une solution différente et consent à un traitement déterminé[147].

Il ne s'agit pas à proprement parler d'un principe dont la violation constitue une atteinte à la personnalité au sens de l'art. 30 al. 2 nLPD, mais bien plus d'une obligation de prendre de mesures techniques et organisationnelles pour assurer le respect des principes et en particulier de celui de la proportionnalité.

M. La communication aux Archives fédérales pour les organes fédéraux

Lorsqu'ils n'ont plus besoin en permanence de données personnelles, les organes fédéraux doivent les proposer aux Archives fédérales

---

145 FF 2017 6649.

146 Cette obligation figure également à l'art. 25 par. 2 RGPD. Voir notamment COMITÉ EUROPÉEN DE LA PROTECTION DES DONNÉES, Guidelines 4/2019 on Article 25 Data Protection by Design and by Default, Version 2.0 du 20 octobre 2020.

147 FF 2017 6649-50.

(art. 38 nLPD)[148]. Ils ne peuvent pas les détruire comme le ferait un responsable du traitement privé.

Si les Archives fédérales les ont désignées comme n'ayant plus de valeur archivistique, l'organe fédéral doit encore s'assurer que ces données personnelles ne doivent pas être conservées à titre de preuve, par mesure de sûreté ou afin de sauvegarder un intérêt digne de protection de la personne concernée. Si tel n'est pas le cas, elles doivent détruites ou conservées seulement après avoir été rendues anonymes.

VI. Les droits de la personne concernée

A. Le droit de savoir et d'emporter ses données

Certains droits de la personne concernée ne sont rien d'autre que l'autre face d'une obligation du responsable du traitement. C'est en particulier le cas du droit de la personne concernée à être informé du traitement de ses données personnelles qui est garanti par le principe de transparence et surtout l'obligation d'information[149].

Ce droit est complété par le droit d'accès[150]. Le droit d'accès est un élément clé du droit de la protection des données car il permet à la personne concernée de faire valoir les droits que lui octroie la loi. C'est un droit subjectif inhérent à la personne, que même une personne qui n'a pas l'exercice des droits civils mais qui est capable de discernement peut faire valoir seule et sans avoir à requérir le consentement de son représentant légal, et auquel il ne peut pas être renoncé valablement par avance[151].

Le droit d'accès consacre premièrement pour toute personne le droit de savoir si des données personnelles la concernant sont traitées (art. 25 al. 1 nLPD)[152]. Il consacre deuxièmement le droit d'en recevoir une copie (art. 25 al. 2 let. b nLPD) et troisièmement celui de recevoir des informations sur l'identité et les coordonnées du responsable du traitement (art. 25 al. 2 let. a nLPD), la finalité du traitement (art. 25 al. 2 let. c nLPD), la durée de conservation ou au moins les critères pour la fixer (art. 25 al. 2 let. d nLPD), les éventuels destinataires ou catégories de destinataires auxquels des données personnelles sont communiquées (art. 25 al. 2 let. g nLPD), les informations disponibles

---

148 Cela correspond à l'art. 21 aLPD.

149 Voir V. A. ci-dessus.

150 Sur le droit d'accès en général, voir Hertig Pea pp 109 ss, Benhamou / D'Errico, di Tria / Lubishtani / Rouiller / Epiney / Pärli / Eggman / Griesinger.

151 FF 2017 6682.

152 Sur la distinction entre droit de savoir et droit d'être renseigné : di Tria / Lubishtani, pp. 29 ss.

sur l'origine des données si elles n'ont pas été collectées auprès de la personne concernée (art. 25 al. 2 let. e nLPD), l'existence éventuelle d'une décision individuelle automatisée ainsi que la logique sur laquelle se base cette décision (art. 25 al. 2 let. f nLPD), la liste des États étrangers vers lesquels les données sont exportées (y compris les garanties appropriées ou les motifs d'exception)[153], et finalement toute autre information nécessaire pour que la personne concernée puisse faire valoir ses droits selon la nLPD et pour que la transparence du traitement soit garantie (art. 25 al. 2 nLPD).

En principe, le responsable du traitement doit répondre dans les 30 jours et gratuitement. Lorsqu'il s'agit de données liées à la santé, il peut les communiquer à la personne concernée par l'intermédiaire d'un professionnel de la santé qu'elle aura désigné[154].

Si le droit d'accès est inconditionnel et ne demande pas de justification, il n'est pas absolu. Dans certains cas, le responsable du traitement peut refuser, restreindre ou différer la communication de renseignements. Il doit néanmoins indiquer à la personne concernée qu'il refuse, restreint ou diffère la communication des informations et le motif invoqué. S'il n'y a pas d'exigences de forme pour les responsables du traitement privés, les organes fédéraux doivent rendre des décisions susceptibles de recours[155].

Plusieurs motifs peuvent être invoqués. Premièrement, une loi formelle peut prévoir que les informations ne doivent pas être communiquées, par exemple pour protéger le secret professionnel (art. 26 al. 1 let. a nLPD). Deuxièmement, la protection des intérêts de tiers, notamment la protection de leur sphère privée, peut s'opposer à la communication (art. 26 al. 1 let. b nLPD). Troisièmement, l'organe fédéral peut invoquer un intérêt public prépondérant, notamment la sûreté intérieure ou extérieure de la Suisse, ou le bon déroulement d'une enquête ou procédure (art. 26 al. 2 let. b ch. 1 et 2 nLPD). Quatrièmement, ce n'est que dans des cas limités (et pas pour cacher un traitement illicite des données) que le responsable du traitement privé peut faire valoir son propre intérêt prépondérant et seulement à la condition que les données ne soient pas transmises à un tiers (art. 26 al. 2 let. a nLPD).

---

153 L'art. 25 al. 2 let. g nLPD prévoit d'une part que le responsable du traitement doit indiquer les destinataires ou les catégories de destinataires auxquels des données personnelles sont communiquées et, d'autre part, les informations prévues à l'art. 19 al. 4 nLPD. C'est ainsi que la liste des États étrangers doit être communiqué à la personne exerçant sa demande de droit d'accès. Conformément à l'art. 19 al. 4 nLPD, et cas échéant, le responsable du traitement doit être communiquer les garanties prévues à l'art. 16 al. 2 nLPD ou les motifs d'exception prévus à l'art. 17 nLPD.

154 L'aLPD permettait, de manière très discutable, de l'imposer à la personne concernée. La nLPD impose désormais à raison le consentement de la personne concernée pour cette remise indirecte. MEIER, N. 1006 ; FF 2017 6684.

155 FF 2017 6686.

Cinquièmement, les médias et journalistes bénéficient de règles particulières pour assurer la liberté de la presse (art. 27 nLPD). Le responsable du traitement peut encore invoquer le principe de l'abus de droit (art. 2 al. 2 CC)[156]. Récemment, le Tribunal fédéral a eu l'occasion de préciser qu'une demande de droit d'accès qui visait à se procurer des preuves en vue d'une procédure civile sans chercher à vérifier les données ou le traitement effectué était abusif[157]. Finalement, le responsable du traitement peut invoquer le caractère manifestement infondé de la demande, notamment parce qu'elle poursuit un but contraire à la protection des données ou qu'elle est manifestement procédurière (art. 26 al. 1 let. c nLPD). C'est le cas d'une demande répétée sans raison mais pas d'une simple marque de curiosité.

L'Assemblée fédérale a introduit le droit à la remise ou à la transmission des données personnelles (art. 28 nLPD), connu en droit européen sous la notion de droit à la portabilité[158]. Ce droit permet à la personne concernée d'obtenir gratuitement les données qu'elle a fourni, voire de les faire remettre directement à un autre responsable du traitement. Les données doivent être remises dans un format électronique courant afin de s'assurer qu'elles pourront être utilisées facilement. Ce droit ne s'applique que si les données sont traitées de manière automatisée et que ce traitement repose soit sur le consentement de la personne concernée, soit qu'il est en relation directe avec la conclusion ou l'exécution d'un contrat entre elle et le responsable du traitement. Si la condition du consentement ou de la nécessité contractuelle a un sens en droit européen (puisqu'il s'agit de deux conditions permettant de justifier un traitement de données, par opposition aux obligations légales ou intérêts du responsable du traitement)[159], elle est très étrange en droit suisse où le consentement n'est requis que s'il y a une atteinte à la personnalité. On peut se demander sérieusement si l'Assemblée fédérale a vraiment voulu exclure du droit à la remise des données traitées sans lien avec un contrat mais dans le respect des principes (pas de consentement nécessaire), mais l'appliquer lorsque les mêmes données sont traitées en violation des principes (ce qui a nécessité un consentement).

---

156 Sur le caractère abusif du droit d'accès, voir ROUILLER / EPINEY, pp. 12 ss.

157 TF 4A_277/2020 du 18 novembre 2020. Contrairement aux ATF 138 III 425 et 141 III 119 où l'intérêt des requérants à vérifier les données, respectivement le traitement, enlevait le caractère abusif du droit d'accès (même s'il ne faisait pas de doute qu'il s'agissait aussi d'une volonté de réunir des preuves).

158 Le droit à la portabilité en droit européen est ancré à l'art. 20 RGPD. Voir notamment REICHLIN, pp. 401 ss ; ROSENTHAL, N. 130 ss ; GROUPE DE TRAVAIL « ARTICLE 29 », Lignes directrices relatives au droit à la portabilité des données du 13 décembre 2016.

159 Art. 6 RGPD.

B. Le droit de s'opposer au traitement ou de faire rectifier les données

La nLPD ne prévoit pas expressément un droit de s'opposer au traitement de données personnelles, mais cela découle du droit à l'autodétermination informationnelle[160]. De plus, le fait de traiter (sans motif justificatif) des données personnelles contre la manifestation expresse de la volonté de la personne concernée constitue une atteinte illicite à la personnalité (art. 30 al. 2 let. b nLPD). Ce droit est donc bien reconnu, mais il peut être limité par une loi ou parfois un intérêt privé ou prépondérant au traitement. De plus, la personne concernée peut exiger qu'une décision individuelle automatisée soit revue par une personne physique (art. 21 al. 2 nLPD)[161].

La personne concernée a le droit de faire rectifier des données erronées la concernant, sauf si la modification est interdite par une disposition légale (art. 32 al. 1 let. a nLPD) ou si les données sont traitées à des fins archivistiques répondant à un intérêt public (art. 32 al. 1 let. b nLPD)[162]. Le droit à la rectification découle directement du principe d'exactitude et il est donc indépendant d'une atteinte à la personnalité[163].

Au lieu d'effacer ou de détruire les données personnelles lorsque la personne s'est opposée au traitement, l'organe fédéral peut limiter le traitement si l'exactitude des données est contestée par la personne concernée et leur exactitude ou inexactitude ne peut pas être établie, si des intérêts prépondérants d'un tiers l'exigent, si un intérêt public prépondérant, en particulier la sûreté intérieure ou extérieure de la Suisse, l'exige, si l'effacement ou la destruction des données est susceptible de compromettre une enquête, une instruction ou une procédure judiciaire ou administrative (art. 41 al. 3 nLPD). La limitation du traitement est une mesure moins radicale que l'effacement ou la destruction des données litigieuses. Cela signifie que le traitement reste possible pour l'organe fédéral, mais uniquement pour les finalités limitées qui ont empêché leur effacement[164].

---

160 Art. 13 Cst, voir notamment FLÜCKIGER, pp. 846 ss (et les nombreuses références citées à la nbp. 76).

161 Sur les concepts de profilage et de décision automatisée, voir HEUBERGER.

162 Les motifs justificatifs de l'art. 31 nLPD ne peuvent pas être invoqués (FF 2017 6693). S'agissant d'un organe fédéral, l'art. 41 al. 2 nLPD prévoit une disposition similaire, étant précisé que la rectification, l'effacement ou la destruction de données personnelles ne peut pas être exigée pour les fonds gérés par des institutions ouvertes au public telles que les bibliothèques, les établissements d'enseignement, les musées, les archives et les autres institutions patrimoniales publiques. Si le demandeur rend vraisemblable qu'il dispose d'un intérêt prépondérant, il peut exiger que l'institution limite l'accès aux données litigieuses (art. 41 al. 5 nLPD).

163 FF 2017 6693. Avis contraire : ROSENTHAL, N. 139.

164 FF 2017 6700.

Dans le cas particulier où ni l'exactitude ni l'inexactitude d'une donnée personnelle ne peut être établie, la personne concernée peut demander que le responsable du traitement ajoute à la donnée la mention de son caractère litigieux[165].

L'exercice judiciaire des droits sera examiné plus loin, mais l'on peut déjà mentionner que la nLPD renvoie encore aux actions classiques des art. 28 ss CC qui s'appliquent en cas d'atteinte à la personnalité. La personne concernée peut ainsi demander l'interdiction d'un traitement déterminé de données ou leur communication à des tiers, ainsi que l'effacement ou la destruction de données personnelles[166]. Le droit à l'effacement correspond dans le domaine de la protection des données au « droit à l'oubli », garanti de manière générale par la protection de la personnalité du droit civil mais rendu célèbre par la CJUE[167]. Finalement, la personne concernée peut aussi obtenir la communication à des tiers ou la publication de la rectification, l'effacement ou la destruction des données, l'interdiction du traitement ou de la communication à des tiers, la mention du caractère litigieux ou encore le jugement[168].

VII. Le traitement illicite

A. Les cas de traitements illicites par des responsables du traitement privés

L'art. 30 al. 2 nLPD prévoit une présomption irréfragable d'atteinte à la personnalité dans trois cas de figure différents : lorsque des données personnelles sont traitées en violation des principes (let. a), lorsque des données personnelles sont traitées contre la manifestation expresse de la volonté de la personne concernée (let. b), ou lorsque des données personnelles sensibles sont communiquées à des tiers (let. c).

L'énumération n'est pas exhaustive et un traitement peut constituer une atteinte à la personnalité même s'il ne figure pas dans la liste de l'art. 30 al. 2 nLPD[169]. La personne concernée devrait alors démontrer dans le cas d'espèce l'existence de l'atteinte et ne bénéficiera pas de la présomption légale.

Ce principe est atténué par l'art. 30 al. 3 nLPD qui précise qu'il n'y a en règle générale pas d'atteinte lorsque la personne concernée a rendu

---

165 Art. 32 al. 3 et 41 al. 4 nLPD.

166 Art. 32 al. 2 et 4 nLPD.

167 FF 2017 6693 et arrêt CJUE Google Spain SL, Google Inc. c. Agencia Española de Protección de Datos (AEPD) et Mario Costeja González, C-131/12 du 13 mai 2014. Voir également Ausloss.

168 Art. 32 al. 4 nLPD.

169 FF 2017 6688.

les données personnelles accessibles à tout un chacun et ne s'est pas opposée expressément au traitement. C'est une présomption légale réfragable de non-atteinte[170]. Le responsable du traitement doit démontrer que les données ont été rendues accessibles à tout un chacun par la personne concernée (consciemment et volontairement), alors que la personne concernée doit démontrer qu'elle s'est opposée formellement au traitement et que cette opposition a bien été reçue[171].

Le premier cas de traitement illicite prévu par la loi concerne la violation des principes figurant aux art. 6 et 8 nLPD et qui doivent guider tout traitement de données[172].

Le deuxième cas de traitement illicite est celui où la personne concernée s'oppose. C'est un droit inconditionnel de s'opposer (*opt-out*) à certains traitements[173]. L'opposition n'est pas soumise à une exigence de forme et n'a pas besoin de justification[174], mais elle doit être expresse[175]. C'est une simple déclaration de volonté soumise à réception[176] qui doit porter sur des auteurs de traitement déterminés ou déterminables. Elle peut porter seulement sur certains traitements ou certaines finalités. Une manifestation de volonté « tacite » comme le fait de ne plus utiliser activement un service n'est pas suffisante[177]. Le droit d'opposition est la concrétisation au plan privé du droit à l'autodétermination informationnelle figurant à l'art. 13 al. 2 Cst[178].

Le troisième cas concerne une situation jugée particulièrement risquée, car il y a le cumul de données sensibles et le transfert à des tiers. Ce double risque justifie de considérer ce traitement comme une atteinte illicite[179].

---

170 FF 2017 6688 ; MEIER, N. 1575.

171 MEIER, N. 1592-1593.

172 La protection des données dès la conception et la protection des données par défaut (art. 7 nLPD) ne sont pas des principes à proprement parler, mais bien plus des obligations à charge du responsable du traitement. Leur violation ne rend pas le traitement illicite au sens de l'art. 30 nLPD ni ne peut être justifiée par un motif de l'art. 31 nLPD.

173 Contrairement au RGPD qui prévoit l'obligation d'avoir un motif justifiant le traitement (souvent le consentement). Il est important de rappeler que le droit suisse n'exige pas toujours un consentement au traitement de données, même de données sensibles (dans le même sens : ROSENTHAL, N. 7).

174 MEIER, N. 1553.

175 MEIER, N. 1559 ; FF 2017 6688.

176 MEIER, N. 1558 ; FF 2017 6688.

177 FF 2017 6688.

178 MEIER, N. 1553.

179 MEIER, N. 15566.

B. Les motifs justificatifs pour les responsables du traitement privés

1. Le principe

Une atteinte à la personnalité est présumée illicite, mais le responsable du traitement peut y opposer des motifs justificatifs. Il faudra alors procéder à une pesée d'intérêts. Une atteinte à la personne est considérée comme licite si elle peut être justifiée par l'un des motifs suivants : le consentement de la personne concernée, un intérêt prépondérant privé, un intérêt prépondérant public, ou par la loi (art. 31 al. 1 nLPD).

2. Le consentement

Le premier motif est le consentement de la personne concernée[180]. Pour qu'il soit valable, la personne concernée doit exprimer librement et clairement sa volonté concernant un ou plusieurs traitements déterminés et après avoir été dûment informée (art. 6 al. 6 nLPD). Il doit être exprès dans les cas d'un traitement de données sensibles ou d'un profilage à risque élevé (art. 6 al. 7 nLPD)[181].

La notion de consentement libre et éclairé vient de la jurisprudence applicable en droit médical[182]. Un consentement est libre si la personne n'a pas subi de menace, de pression déraisonnable, directe ou indirecte (de la part du responsable du traitement ou d'un tiers).

Subir un désavantage en l'absence de consentement ne signifie pas forcément que le consentement n'est pas libre, mais le consentement ne sera pas libre si le désavantage est sans rapport avec le but du traitement ou manifestement disproportionné[183]. Il n'est pas obligatoire de fournir une alternative pour que le consentement puisse être libre[184], mais s'il y a une alternative, c'est un fort indice de liberté de consentir.

La liberté de consentement présuppose aussi que les informations qui ne sont pas obligatoires soient présentées comme telles[185].

Le consentement est éclairé si la personne concernée a reçu une information objective, complète et compréhensible sur le traitement envisagé, en particulier sur le responsable du traitement, les finalités, le type

---

180 Sur la notion de consentement en protection des données, voir notamment FASNACHT.

181 Lorsque le consentement est requis, il doit être exprès seulement pour un profilage à risque élevé effectué par une personne privée. Si le profilage est l'œuvre d'un organe fédéral, le consentement doit être exprès qu'il s'agisse d'un profilage simple ou à risque élevé.

182 MEIER, N. 831.

183 MEIER, N. 853.

184 MEIER, N. 859.

185 MEIER, N. 705, 852, 861.

et l'étendue des données traitées, les opérations de traitement envisagées, etc.[186] La personne doit donc disposer de tous les éléments qui au vu des circonstances, lui permettent de prendre une décision en toute connaissance de cause.

Le consentement devrait être donné par un acte positif clair par lequel la personne concernée manifeste de façon libre, spécifique, éclairée et univoque son accord au traitement. L'expression du consentement peut se faire par oral ou par écrit, y compris en cochant une case lors de la consultation d'un site web. Il n'y a en revanche pas de consentement en cas de silence, de cases cochées par défaut ou d'inactivité[187].

3. L'intérêt privé

Le deuxième motif est l'intérêt privé prépondérant. Pour la prévisibilité du droit, l'art. 31 al. 2 nLPD dresse une liste non exhaustive d'intérêts qui sont en principe reconnus comme prépondérants. C'est le plus souvent l'intérêt du responsable du traitement, mais parfois aussi de la personne concernée ou d'un tiers. Le juge doit procéder à chaque fois à une pesée d'intérêts dans le cas d'espèce entre l'intérêt du responsable du traitement au traitement et l'intérêt de la personne concernée au non-traitement[188].

Si l'intérêt de la personne concernée est *per se* digne de protection (protection de sa personnalité), il faut déterminer l'intérêt du responsable du traitement et vérifier s'il est digne de protection (légitime). On procédera ensuite à la pesée d'intérêts.

Il n'y a guère de changement dans la nLPD parmi les principaux intérêts prépondérants du responsable du traitement. Ainsi, la liste correspond pour l'essentiel à celle qui est en vigueur. On retrouve donc l'hypothèse où le traitement est en relation directe avec la conclusion ou l'exécution d'un contrat, pour autant que les données traitées concernent le cocontractant (art. 31 al. 2 let. a nLPD). On retrouve également le cas selon lequel le traitement s'inscrit dans un rapport de concurrence actuel ou futur avec une autre personne, pour autant que les données ne soient pas communiquées à des tiers (art. 31 al. 2 let. b nLPD). S'agissant des données personnelles traitées de manière professionnelle exclusivement en vue d'une publication dans la partie rédactionnelle d'un média à caractère périodique, ou qui servent exclusivement d'instrument de travail personnel si la publication n'a pas lieu, ce cas est prévu à l'art. 31 al. 2 let. d nLPD. Finalement, le cas des données personnelles

---

186 MEIER, N. 861.

187 C. 32 RGPD. À ce propos, voir COMITÉ EUROPÉEN DE LA PROTECTION DES DONNÉES, Lignes directrices 5/2020 sur le consentement au sens du RGPD du 4 mai 2020.

188 MEIER, N. 1609 ; FF 2017 6689.

recueillies concernant une personnalité publique et se référant à son activité publique est à nouveau ancré dans la loi, à l'art. 31 al. 2 let. f nLPD.

À certaines conditions, les données personnelles traitées dans le but d'évaluer la solvabilité de la personne concernée représentent aussi un intérêt prépondérant (art. 31 al. 1 let. c nLPD)[189]. Après de nombreuses discussions, l'Assemblée fédérale a finalement décidé que ces données, qui ne doivent représenter ni des données sensibles ni un profilage à risque élevé, ne doivent pas dater de plus de dix ans et ne pas concerner des personnes mineures. Les données ne peuvent être communiquées à des tiers que s'ils en ont besoin pour conclure ou exécuter un contrat avec la personne concernée.

Finalement, il y a un intérêt large dans le cadre de la recherche, de la planification ou de la statistique[190]. Des données personnelles peuvent y être traitées pour autant qu'elles le soient à des fins ne se rapportant pas à des personnes. Le responsable du traitement doit en outre les anonymiser dès que possible[191], ne pas communiquer à des tiers des données sensibles sous une forme permettant d'identifier la personne concernée et ne pas publier de résultats sous une forme permettant d'identifier les personnes concernées.

4. L'intérêt public

Le troisième motif, l'intérêt public prépondérant, est assez rare, car il est généralement déjà repris dans une loi. Il n'est pas défini par la nLPD, mais on peut retenir qu'il y a un intérêt public lorsque l'atteinte est destinée à procurer un avantage à la collectivité ou au moins à une pluralité de personnes[192].

L'intérêt public prépondérant peut aussi intervenir en soutien d'un intérêt privé. C'est par exemple le cas de l'intérêt d'une assurance privée à ne pas servir des prestations indues ainsi que celui de la collectivité des assurés à ne pas voir les coûts de leurs assurances augmenter[193].

---

189 ROSENTHAL, N. 42 ; FF 2017 6690-6691.

190 L'art. 39 nLPD prévoit que les organes fédéraux peuvent également traiter des données à des conditions similaires sans devoir respecter les principes de finalité et de base légale.

191 Cette condition est déjà réalisée lorsque les données sont communiquées sous une forme pseudonymisée et que la clé pour réidentifier la personne reste chez celui qui transmet les données (FF 2017 6692).

192 MEIER, N. 1612 ss.

193 ATF 136 III 410, c. 2.2.3.

5. La loi

Le quatrième motif justificatif est une disposition légale de droit fédéral ou cantonal, qui impose le traitement, le permet ou le suppose en lien avec d'autres obligations qu'elle prévoit[194]. Lorsque la loi sert de motif justificatif, cela signifie que le législateur a déjà procédé à une pesée d'intérêts. C'est par exemple le cas de l'examen de la capacité de contracter un crédit (art. 23 ss LCC), de l'obligation de conserver les pièces comptables (art. 957 et 962 CO, ainsi que l'OLICO) et de l'enregistrement de conversations téléphoniques lors de commandes (art. 179^{quinquies} CP).

C. Les traitements illicites par les organes fédéraux

La nLPD et en particulier le chapitre 6 ne prévoient pas de règles spécifiques sur le traitement illicite. Un traitement de données par l'administration fédérale est néanmoins illicite lorsque les données sont traitées en violation des principes[195] ou d'autres prescriptions de la nLPD, ou lorsque les données sont traitées en l'absence d'une base légale (art. 34 nLPD)[196] ou en violation de cette base légale.

VIII. L'EXERCICE JUDICIAIRE DES DROITS ET LA SAISINE DU PRÉPOSÉ

La nLPD impose des obligations aux responsables du traitement pour garantir le respect des principes et des droits des personnes concernées. Les moyens d'action à disposition des personnes concernées dépendent du responsable du traitement. La nLPD prévoit très largement que la personne concernée doit agir par la voie civile si le responsable du traitement est une personne privée ou par la voie d'un recours contre la décision rendue par l'organe fédéral responsable, pour faire valoir ses droits[197].

Lorsque l'on parle de l'exercice des droits devant la justice civile, on pense surtout aux actions en cas d'atteinte à la personnalité des art. 28 ss CC et 32 nLPD mentionnées ci-dessus[198], mais la personne concernée peut aussi saisir la justice pour obtenir un droit d'accès qui lui serait refusé[199]. Elle peut également faire valoir des moyens réparateurs

---

194 MEIER, N. 1601.

195 Art. 30 al. 2 nLPD par analogie.

196 Mais également art. 13 al. 2 et 36 Cst, ainsi que 8 CEDH.

197 FF 2017 6705.

198 HERTIG PEA pp. 123 ss.

199 Voir notamment BENHAMOU, pp. 77 ss.

tels que des prétentions en réparation du dommage subi (art. 41 et 97 CO), y compris le tort-moral (art. 49 CO), voire en remise de gain (421 al. 1 CO)[200]. S'agissant d'un organe fédéral, la procédure est régie par la Loi fédérale sur la procédure administrative (PA) mais l'art. 41 nLPD prévoit des dispositions similaires.

Les dispositions pénales que contient la nLPD sont assez limitées et concernent surtout la violation des obligations d'informer, de renseigner et de collaborer (art. 60 nLPD), ainsi que la violation des devoirs de diligence par le responsable du traitement (art. 61 nLPD) et la violation du devoir de discrétion (art. 62 nLPD). Ces infractions sont poursuivies seulement sur plainte. Toute personne lésée pouvant déposer plainte (art. 30 CP), il faudra admettre assez largement que toute personne qui n'a pas reçu les informations qu'elle aurait dû recevoir ou dont les données sont traitées sans respecter les devoirs de diligence a qualité pour déposer plainte. L'art. 65 al. 2 nLPD prévoit également que le PFPDT peut dénoncer des infractions aux autorités de poursuite pénale compétentes et faire valoir les droits d'une partie plaignante dans la procédure.

Il pourra aussi dénoncer les responsables du traitement qui, intentionnellement, ne se conforment pas à une décision qu'il leur a été signifiée sous la menace de la peine prévue à l'art. 63 nLPD. L'insoumission à cette décision serait alors une contravention, poursuivie d'office, et passible d'une amende pénale de 250'000 francs au maximum. Lorsque la décision du PFPDT s'adresse à une entreprise, c'est une personne physique occupant une fonction dirigeante qui sera punissable[201]. À noter que les contraventions pénales ne visent que les responsables du traitement privés et pas les organes fédéraux.

Qu'il s'agisse d'un responsable du traitement privé ou d'un organe fédéral, la personne concernée peut saisir le PFPDT, qui est tenu d'ouvrir une enquête d'office ou sur dénonciation dès que des indices font penser que des traitements de données pourraient être contraires à des dispositions légales de protection des données (art. 49 al. 1 nLPD). Le dénonciateur, même si c'est la personne concernée, n'a pas qualité de partie à la procédure (art. 52 al. 2 nLPD *a contrario*). Il sera toutefois informé de la suite donnée à sa dénonciation (art. 49 al. 4 nLPD).

Malheureusement, et contrairement à ce qui prévaut en droit européen, le PFPDT n'a pas le pouvoir d'infliger des sanctions administratives, et encore moins des amendes. À l'issue de son enquête, le PFPDT peut seulement prononcer un certain nombre de mesures administratives

---

200 MEIER, N. 1774.

201 Art. 29 CP ; FF 2017 6718.

qui, en cas de non-respect, pourraient être sanctionnées pénalement[202]. Il n'a toutefois pas l'obligation de le faire.

Ces mesures concernent d'abord des traitements de données contraires à des dispositions de protection des données. Cela va du simple avertissement jusqu'à l'ordre de cesser le traitement ou de détruire des données personnelles (art. 51 al. 1 et 5 nLPD). Le PFPDT peut aussi interdire la communication de données personnelles à l'étranger (art. 51 al. 2 nLPD). Le principe de proportionnalité doit dans tous les cas être respecté.

Des mesures peuvent ensuite être prises en cas de non-observation de prescriptions d'ordre ou de devoirs à l'égard de la personne concernée (art. 51 al. 3 et 4 nLPD). Le PFPDT peut, par exemple, ordonner à l'organe fédéral ou au responsable du traitement privé de prendre des mesures techniques et organisationnelles, d'établir une analyse d'impact et de le consulter, d'annoncer une violation de la sécurité, de communiquer les informations requises en matière de transfert à l'étranger ou de désigner un représentant.

Le responsable du traitement privé et l'organe fédéral peuvent évidemment recourir contre la décision du PFPDT.

IX. Conclusions

Le chemin qui a conduit à l'adoption de la nLPD a été inutilement long et compliqué. La version qui sera applicable en Suisse 30 ans après l'adoption de l'aLPD n'a pourtant rien de révolutionnaire. Elle renforce un peu les droits des personnes concernées, mais sans accorder de droits de recours ou de représentation collectifs. Elle renforce également un peu les pouvoirs du PFPDT qui pourra (enfin) rendre des décisions, mais sans pour autant prononcer d'amendes. La crainte des milieux économiques d'être régulés a été très forte, alors que c'était aussi dans leur intérêt. La nLPD renforce encore les obligations du responsable du traitement, mais sans être trop formaliste non plus, et c'est ici à saluer.

De nombreuses institutions sont reprises du RGPD et de la Convention 108 modernisée, mais sans les reprendre toujours à l'identique. Par exemple l'annonce des violations de la sécurité des données doit avoir lieu dans les meilleurs délais selon la nLPD et dans les meilleurs délais mais si possible 72 heures au plus tard après selon le RGPD. Il sera intéressant de voir si la nLPD sera interprétée comme le RGPD (dans notre exemple en introduisant par la bande la notion de 72 heures), ou comme un texte autonome qui a voulu expressément s'écarter du RGPD (et ne surtout pas considérer que la notion de meilleurs délais se rapproche de 72 heures). Il n'y a probablement pas de réponse générale et

---

202 FF 2017 6708.

cela dépendra des articles concernés, mais cela risque surtout d'apporter pendant encore quelque temps plus d'incertitudes que de clarté.

Finalement, et même lorsque la nLPD est moins stricte que le RGPD, de nombreux responsables du traitement appliqueront spontanément le RGPD, soit parce qu'ils n'ont pas attendus la nLPD, soit pour éviter d'avoir des règles trop différentes selon les clients dont les données sont traitées. Quant à ceux qui ne sont pas encore en règle avec l'aLPD, il va sans dire que le travail de mise en conformité sera important et qu'il ne faut plus attendre.

Selon que l'on voit le verre à moitié vide ou à moitié plein, on peut retenir que la nLPD est une occasion manquée d'avoir sensiblement amélioré le niveau de protection des résidents suisses (et qu'il faudra encore attendre un moment), ou alors que l'on a rattrapé le gros du retard et que la loi est presque à jour avec l'état actuellement de la technologie. Tout est question de perspective.

———

BIBLIOGRAPHIE

Sauf indication contraire, les ouvrages ou articles de cette bibliographie sont cités dans les notes avec l'indication du seul nom de l'auteur ou des auteurs.

AUSLOOS JEF, The Right to Erasure in EU Data Protection Law : From Individual Rights to Effective Protection, Oxford 2020

BAERISWYL BRUNO / PÄRLI KURT (édit.), Hankommentar Datenschutzgesetz (DSG), Berne 2015 (cité : SHK DSG-AUTEUR)

BELSER EVA MARIA / EPINEY ASTRID / WALDMANN BERNHARD (édit.), Datenschutzrecht – Grundlagen und öffentliches Recht, Berne 2011

BENHAMOU YANIV, Mise en œuvre judiciaire du droit d'accès LPD – aspects procéduraux choisis, in : Métille (édit.), Le droit d'accès, pp. 77 ss

CAVOUKIAN ANN, Privacy by Design – The 7 Foundational Principles, 2009 (disponible en ligne sur le site du Commissaire à l'information et à la protection de la vie privée de l'Ontario : https://www.ipc.on.ca/wp-content/uploads/Resources/7foundationalprinciples.pdf [consulté le 01.01.2021])

D'ERRICO LUCA, Répondre à une demande de droit d'accès – aspects pratiques, in : Métille (édit.), Le droit d'accès, pp. 107 ss

DI TRIA LIVIO, L'analyse d'impact relative à la protection des données (AIPD) en droit européen et suisse, in : sic ! 3/2020, p. 119 ss

DI TRIA LIVIO / LUBISHTANI KASTRIOT, Étude empirique du droit d'accès à ses données personnelles, in : Métille (édit), Le droit d'accès, pp. 29 ss

FASNACHT TOBIAS, Die Einwilligung im Datenschutzrecht, thèse Fribourg, Zurich/Bâle/Genève 2017

FLÜCKIGER ALEXANDRE, L'autodétermination en matière de données personnelles : un droit (plus si) fondamental à l'ère digitale ou un nouveau droit de propriété ? in : Pratique juridique actuelle. 2013, vol. 22, N. 6, pp. 837-864

GRIESINGER MARCEL, Der datenschutzrechtliche Auskunftsanspruch nach Art. 15 DSGVO, in : Jusletter du 20 janvier 2020

HERTIG PEA AGNÈS, La protection des données personnelles médicales est-elle efficace ? – Étude des moyens d'action en droit suisse, thèse Neuchâtel, Bâle 2013

HEUBERGER OLIVIER, Profiling im Persönlichkeits- und Datenschutzrecht der Schweiz, thèse Lucerne, Zurich/Bâle/Genève 2020

KUNER CHRISTOPHER / BYGRAVE LEE A. / DOCKSEY CHRISTOPHER (édit.), The EU General Data Protection Regulation (GDPR) – A commentary, Oxford 2019 (cite : AUTEUR, in : KUNER / BYGRAVE / DOCKSEY)

KÜHLING JÜRGEN / BUCHNER BENEDIKT, Datenschutz-Grundverordnung/ Bundesdatenschutzgesetz Kommentar, 3e éd., Munich 2020 (cité: AUTEUR, in : KÜHLING / BUCHNER)

MAURER-LAMBROU URS / BLECHTA GABOR-PAUL, Datenschutzgesetz (DSG)/Öffentlichkeitsgesetz (BGÖ), Basler Kommentar, 3e éd., Bâle 2014 (cité : BSK DSG-AUTEUR)

MEIER PHILIPPE, Protection des données – Fondements, principes généraux et droit privé, Berne 2011

PÄRLI KURT / EGGMANN JONAS, Das Auskunftsrechts im Privatrecht, in : digma 2020.3, pp 140-151

REICHLIN JEREMY, Le droit à la portabilité des données sous le RGPD, in : Molin-Kränzlin / Schneuwly / Stojanovic (édit.), Digitalisierung – Gesellschaft – Recht, pp. 401 ss

ROSENTHAL DAVID, Das neue Datenschutzgesetz, in : Jusletter du 16 novembre 2020

ROSSI JULIEN, Protection des données personnelles et droit à la vie privée : enquête sur la notion controversée de « donnée à caractère personnel », Thèse, Compiègne 2020

ROUILLER FÉLISE / EPINEY ASTRID, Le droit d'accès à ses données personnelles, in : Métille (édit.), Le droit d'accès, pp. 1 ss

THOUVENIN FLORENT / GLATTHAAR MATTHIAS / HOTZ JULIETTE / ETTLINGER CLAUDIUS / TSCHUDN MICHAEL, Privacy Icons : Transparenz auf einen Blick, in : Jusletter du 30 novembre 2020

TABLE DES MATIÈRES

I. INTRODUCTION 1
A. Le contexte 1
B. Les principales différences 3

II. LE CHAMP D'APPLICATION 4
A. Des données personnelles… 4
B. … traitées par des privés et organes fédéraux… 6

III. LES ACTEURS 7

IV. LES PRINCIPES 8
A. La bonne foi 8
B. La licéité 8
C. La proportionnalité 9
D. La finalité 10
E. La transparence 11
F. L'exactitude 11
G. La sécurité 12

V. LES OBLIGATIONS DU RESPONSABLE DU TRAITEMENT 13
A. L'information 13
B. Le registre des activités de traitement 16
C. Le représentant 17
D. Le conseiller à la protection des données. 18
E. La sous-traitance 19
F. Le transfert à l'étranger 20
G. L'analyse d'impact relative à la protection des données personnelles 22
H. L'annonce des violations de la sécurité des données 24
I. Le profilage à risque élevé 26
J. La décision individuelle automatisée 27
K. La protection des données dès la conception 28
L. La protection des données par défaut 29
M. La communication aux Archives fédérales pour les organes fédéraux 29

VI. LES DROITS DE LA PERSONNE CONCERNÉE 30
A. Le droit de savoir et d'emporter ses données 30
B. Le droit de s'opposer au traitement ou de faire rectifier les données 33

VII. LE TRAITEMENT ILLICITE 34
A. Les cas de traitements illicites par des responsables du traitement privés 34
B. Les motifs justificatifs pour les responsables du traitement privés 36
1. Le principe 36
2. Le consentement 36
3. L'intérêt privé 37
4. L'intérêt public 38
5. La loi 39
C. Les traitements illicites par les organes fédéraux 39

VIII. L'EXERCICE JUDICIAIRE DES DROITS ET LA SAISINE DU PRÉPOSÉ 39

IX. CONCLUSIONS 41

BIBLIOGRAPHIE 43