Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Département fédéral de justice et police (DFJP)
Office fédéral de la justice (OFJ)
Domaine de direction Droit public
Unité Projets législatifs I

Octobre 2022

Révision totale de la loi fédérale sur la protection des données (LPD)

Aperçu des principales modifications en vue de l'élaboration des bases légales concernant le traitement de données par les organes fédéraux

La révision totale de loi fédérale sur la protection des données (ci-après « nLPD ») doit assurer l'adaptation de la protection des données aux développements technologiques et rapprocher le niveau de protection suisse des exigences européennes. La nLPD reste une loi-cadre et une loi transversale. Elle fixe les exigences relatives au traitement des données, ainsi que les mesures mises en place au niveau des institutions, de l'organisation et du droit de procédure pour assurer le respect des principes de la protection des données. La conception concrète du traitement des données dans le domaine du droit public au niveau fédéral continue cependant à être définie essentiellement dans les réglementations spéciales. La nLPD définit les exigences générales, une grande partie des principes fondamentaux restant inchangés. La révision totale de la LPD introduit toutefois une série de nouveautés, dont il faudra tenir compte dans les projets législatifs (par ex. le « profilage » ou les « décisions individuelles automatisées »).

Le présent document reprend et approfondit les modifications les plus importantes, en vue de l'élaboration des bases légales du traitement des données par les organes fédéraux. Il complète les explications de base figurant dans le Guide de législation (chapitre 14 ; ch. 813 ss) et dans le « Guide de législation en matière de protection des données ». Il s'adresse en premier lieu aux personnes chargées d'élaborer des bases légales et qui, pour leur projet législatif, souhaitent connaître en détail les dispositions de la nLPD.

Le document contient un aperçu des éléments clés et des documents de la révision totale de la LPD (► point 1). Il relève ensuite les principes de protection des données et de légistique qui restent inchangés malgré la révision totale de la LPD (► point 2.1). La partie principale présente les modifications les plus importantes introduites par la révision, s'agissant des exigences en matière de niveau et de densité des normes des bases légales spéciales applicables au traitement de données personnelles par des organes fédéraux (► point 2.2). Un chapitre séparé est consacré au traitement des données de personnes morales, qui sont exclues du champ d'application de la loi révisée (► point 3). Le dernier chapitre survole un certain nombre d'autres nouveautés introduites par la révision totale de la LPD et qui peuvent être pertinentes pour des projets législatifs (► point 4).

BJ-D-12643401/222

Table des matières

1 Éléments clés de la révision totale de la LPD

Le Parlement a divisé le projet du Conseil fédéral du 15 septembre 2017 concernant la révision totale de la LPD (P-LPD) en deux étapes :

- La **première étape** a consisté uniquement à mettre en œuvre la directive UE 2016/680 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, ci-après directive UE 2016/680 relative à la protection des données dans le domaine pénal (développement de l'acquis de Schengen). À cet effet et à titre provisoire, une nouvelle loi sur la protection des données Schengen (LPDS ; RS 235.3) a été élaborée, laquelle est entrée en vigueur le 1er mars 2019[1]. Cette loi contient les dispositions cadres relatives à la protection des données en rapport avec la coopération Schengen en matière pénale, dans la mesure où la LPD en vigueur ne satisfait pas aux exigences de la directive UE 2016/680. En plus de la LPDS, différentes dispositions sur la protection des données dans d'autres lois fédérales qui sont pertinentes pour la coopération policière et judiciaire (notamment code pénal [CP ; RS 311.0] et loi sur l'entraide pénale internationale [RS 351.1]) ont été adaptées ou complétées. L'entrée en vigueur de la LPD révisée entraînera l'abrogation de la LPDS, dans la mesure où les normes de protection de la directive de l'UE 2016/680 seront couvertes par la nouvelle loi. En revanche, les adaptations dans le droit sectoriel demeurent en vigueur.

- La **deuxième étape** a consisté en la « révision totale » de la LPD à proprement parler. Cette révision met notamment en œuvre les exigences de la Convention 108+ pour la protection des personnes à l'égard du traitement des données à caractère personnel du Conseil de l'Europe[2]. En outre, elle rapproche le droit suisse en matière de protection des données du règlement général de l'UE 2016/679 sur la protection des données, afin que le niveau de protection des données attesté pour la Suisse reste suffisant (on parle de « décision d'adéquation »). Le Parlement a approuvé la révision totale de la LPD le 25 septembre 2020. Le délai référendaire a expiré le 14 janvier 2021 sans qu'aucune demande de référendum n'ait été déposée.

1.1 Documentation relative à la révision totale de la LPD

- **Texte de la nLPD soumis au vote final** du 25 septembre 2020 : FF **2020** 7397 / BBl **2020** 7639
- **Bulletin officiel**
- **Curia Vista :** les documents soumis au Parlement, les dépliants et la chronologie sont consultables sous le numéro d'objet 17.059.
- **Message et projet du Conseil fédéral** du 15 septembre 2017 : FF **2017** 6565 et **2017** 6803 / BBl **2017** 6941 et **2017** 7193

[1] Voir le rapport explicatif de l'OFJ d'octobre 2018 concernant la loi fédérale mettant en œuvre 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 prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales (à consulter sous <https://www.bj.admin.ch/bj/fr/home/staat/gesetzgebung/datenschutzstaerkung.html>).

[2] La Suisse n'a pas encore ratifié la Convention 108+ du Conseil de l'Europe pour la protection des personnes à l'égard du traitement des données à caractère personnel. Le Conseil fédéral a toutefois signé le protocole d'amendement correspondant le 21 novembre 2019. Le 19 juin 2020, le Parlement a approuvé, à une forte majorité, l'arrêté fédéral portant approbation de la Convention 108+ (numéro de l'objet 19.068). La révision totale de la LPD met en œuvre les exigences de la Convention 108+ au niveau fédéral. La ratification de cette convention ou l'adhésion de la Suisse ne sera possible que lorsque la nouvelle loi sur la protection des données sera entrée en vigueur.

- **Autres documents** : les documents des stades précédents du projet, par exemple l'avant-projet, les résultats de la procédure de consultation ou les rapports d'experts sont tous accessibles depuis la page internet de l'OFJ « Renforcement de la protection des données ».

1.2 Perspectives : adaptation d'ordonnances et entrée en vigueur de la nouvelle législation sur la protection des données

- Dans le sillage de la révision de la LPD, l'ordonnance relative à la loi fédérale sur la protection des données (**OLPD** ; nouveau : ordonnance sur la protection des données, OPDo) et l'ordonnance sur les certifications en matière de protection des données (**OCPD**) doivent également être adaptées. À l'annexe 2 de l'OPDo, de nombreuses dispositions spéciales sur la protection des données ont été modifiées. Ces **modifications d'autres ordonnances** se limitent aux adaptations découlant directement de la nLPD ou des révisions de l'OLPD ou de l'OCPD (par ex. suppression ou remplacement de la notion de « profil de la personnalité » ► point 2.2.1, let. b), ou adaptation de la notion de « fichier [de données personnelles] » ► point 4.4.2).

- **Principal contenu de la révision de l'OLPD** : exigences minimales en matière de sécurité des données ; sous-traitance de données ; communication de données personnelles à l'étranger (y compris liste des États garantissant un niveau de protection des données adéquat) ; modalités de différentes obligations incombant aux responsables du traitement (notamment devoir d'informer, analyse d'impact relative à la protection des données personnelles et annonce des violations de la sécurité des données) ; modalités du droit d'accès et du droit à la remise ou à la transmission de données [portabilité des données] ; désignation des conseillères et conseillers à la protection des données, définition de leurs tâches et de leur position ; annonce au PFPDT des projets d'organes fédéraux prévoyant le traitement automatisé de données personnelles ; devoir d'informer ; essais pilotes ; organisation et tâches du Préposé fédéral à la protection des données et à la transparence (PFPDT).

- **Entrée en vigueur du nouveau droit sur la protection des données** : en vertu de l'art. 74, al. 2, nLPD, c'est le Conseil fédéral qui fixe la date de l'entrée en vigueur de la LPD révisée (et des ordonnances révisées). Le nouveau droit de la protection des données entrera en vigueur le 1er septembre 2023.

2 Exigences de la révision totale de la LPD pour les bases légales relatives au traitement de données personnelles par des organes fédéraux

2.1 Ce qui *n'est pas modifié* par la révision totale de la LPD

- **Principes de protection des données** : les principes généraux régissant la protection des données de personnes physiques (= données personnelles ; pour les données de personnes morales, voir ► point 3), fixés aux art. 6 à 8 nLPD, doivent être respectés lors du traitement par des organes fédéraux. Les principes fondamentaux de la licéité (art. 6, al. 1, nLPD), de la proportionnalité (y compris la minimisation des données) et de la bonne foi (art. 6, al. 2 et 4 nLPD), de la finalité[3] et de la reconnaissabilité[4] (art. 6, al. 3 nLPD), de l'exactitude des données (art. 6, al. 5, nLPD)[5] ainsi que de la sécurité des données (art. 8 nLPD) correspondent pour l'essentiel au droit en vigueur. L'art. 7 nLPD introduit le principe de la protection des données par la mise en place de mesures techniques et organisationnelles (« protection des données dès la conception et par défaut »). Le principe de la protection des données dès la conception requiert que le traitement de données soit conçu d'entrée, sur les plans de l'organisation et de la technique, de manière que les prescriptions en matière de protection des données soient respectées (art. 7, al. 1, nLPD). Le principe de la protection des données par défaut exige en revanche que des réglages préalables assurent que le traitement des données soit limité au minimum requis par la finalité poursuivie, à moins que la personne concernée n'en ait disposé autrement (art. 7, al. 3, nLPD). Les deux principes découlent en partie des principes de proportionnalité et de sécurité des données fixés dans la législation actuelle. Pour la communication de données à l'étranger, il convient de tenir compte en outre des art. 16 et 17 nLPD (► point 4.2).

- **Principe de l'habilitation spéciale** : la nLPD n'habilite pas d'une manière générale les organes fédéraux à traiter des données — à quelques rares exceptions près —, mais exige des bases légales spécifiques par domaine. En d'autres termes, lorsque des organes fédéraux traitent des données personnelles, les bases légales nécessaires doivent être créées dans des actes normatifs correspondants, pour lesquels la nLPD définit différentes exigences.

- **Exigence d'une base légale** : les organes fédéraux n'ont le droit de traiter des données personnelles que s'il existe une base légale (art. 34, al. 1, nLPD). Cette règle s'applique à toutes les formes et toutes les phases du *traitement des données* (art. 5, let. d, nLPD), par exemple la collecte, l'utilisation, la conservation ou l'effacement des données (« cycle de vie » des données personnelles). La *communication de données* (art. 5, let. e, nLPD), qui est une forme particulièrement sensible de traitement des données, est régie par l'art. 36

---

[3] La formulation du principe de la finalité à l'art. 6, al. 3, nLPD s'écarte légèrement du libellé actuel (art. 4, al. 3, LPD). Il est désormais fixé explicitement que les données ne peuvent être traitées que d'une manière **compatible** avec le but initial de leur collecte. Il est précisé dans le message du Conseil fédéral du 15 septembre 2017 (► FF **2017** 6565, 6645) que la nouvelle formulation n'implique pas de changements majeurs : comme aujourd'hui, un traitement ultérieur ne sera pas admissible si la personne concernée peut légitimement le considérer comme inattendu, inapproprié ou contestable. Une modification de la finalité initiale d'un traitement de données par des organes fédéraux doit donc d'une manière générale être prévue par la loi. Le principe de la finalité doit également être respecté dans le cadre des projets de l'administration fédérale prévoyant l'utilisation multiple de données (« principe de la collecte unique des données » ou, en anglais, principe du « only once »).

[4] Même si le principe de la reconnaissabilité prévu à l'art. 6, al. 3, nLPD s'écarte légèrement de la formulation du droit en vigueur (art. 4, al. 4, LPD), il est indiqué dans le message du Conseil fédéral du 15 septembre 2017 (► FF **2017** 6565, 6645) – et contrairement à des avis divergents (notamment DAVID ROSENTHAL, La nouvelle loi sur la protection des données, in : Jusletter du 16 novembre 2020, ch. 35) – qu'il n'y a cependant aucun changement matériel.

[5] Les deux premières phrases de l'art. 6, al. 5, nLPD disposent que toute personne qui traite des données personnelles doit s'assurer qu'elles sont exactes et doit prendre toute mesure appropriée permettant de rectifier, d'effacer ou de détruire les données inexactes ou incomplètes au regard des finalités pour lesquelles elles sont collectées ou traitées. Cette teneur correspond à celle de l'actuel art. 5, al. 1, LPD. Dans la *troisième phrase* de l'art. 6, al. 5, nLPD, le Parlement a précisé que le caractère approprié de la mesure dépend notamment du type de traitement et de son étendue, ainsi que du risque que le traitement des données en question présente pour la personnalité ou les droits fondamentaux des personnes concernées. Ce complément inscrit explicitement dans la loi l'acception de l'« exactitude des données » selon la doctrine et la pratique (en particulier du Tribunal administratif fédéral). Il n'y a cependant aucune intention de changer la teneur de cette disposition.

nLPD. Les organes fédéraux ont besoin d'une base légale spécifique pour la communication de données (autrement dit, une compétence générale à traiter des données ne suffit pas). Cependant, les exigences auxquelles doit satisfaire la base légale sont en grande partie identiques à celles qui sont fixées pour d'autres formes de traitement des données (renvoi de l'art. 36, al. 1, nLPD à l'art. 34, al. 1 à 3, nLPD).

- **Exigences concernant le niveau normatif :** la règle générale est que plus l'atteinte au droit d'être protégé contre l'emploi abusif de données personnelles est grave (art. 13, al. 2, Constitution fédérale [Cst. ; RS 101])[6], plus il sera nécessaire de disposer d'une base légale dans une loi au sens formel. Comme jusqu'ici, le législateur détermine lui-même un certain nombre de cas dans lesquels une loi au sens formel est requise (art. 34, al. 2, et art. 36, al. 1, nLPD). Il y a cependant quelques modifications à relever par rapport au droit actuel (► point 2.2.1).

- **Exigences concernant la densité normative :** la base légale pour le traitement des données doit présenter une précision suffisante. Ni la LPD en vigueur, ni la nLPD ne contiennent de dispositions particulières à ce sujet. Les exigences concernant la densité normative obéissent donc d'une manière générale au principe de la légalité, c'est-à-dire qu'elles dépendent du risque que présente un traitement de données. La base légale doit être d'autant plus détaillée que l'ingérence dans le droit à l'autodétermination informationnelle est grande. Les critères suivants sont particulièrement déterminants : le type de données, le mode et la finalité du traitement, le nombre et le cercle de personnes concernées, l'éventuelle association d'autres entités au traitement des données (organes fédéraux, organes cantonaux ou bureaux privés) ou le recours à de nouvelles technologies.

  La règle générale est la suivante : la base légale doit assurer la transparence du traitement des données par les organes fédéraux. Dans les cas énoncés à l'art. 34, al. 2, nLPD (en relation avec l'art. 36, al. 1, nLPD), les personnes concernées doivent reconnaître clairement dans la loi formelle, *qui* (► point 4.1) traitera *quelles données*, *à quelles fins*, et *à qui* elles seront communiquées *dans quel but*, et *de quelle manière* les données seront traitées. Par mode de traitement des données, on entend par exemple les méthodes telles que la mise en relation ou le rapprochement de données (y compris le profilage ; voir ► point 2.2.1 let. b)) ou le recours à de nouvelles technologies (par ex. procédés biométriques ou intelligence artificielle ; voir ► point 2.2.1, let. c)/cc) ainsi que la durée de conservation des données dans le cas d'atteintes graves aux droits fondamentaux. Pour les modalités de la communication des données, voir aussi ► point 2.2.2.

  Ces dernières années, la question s'est posée de plus en plus souvent de savoir s'il fallait spécifier dans la base légale l'*architecture du système* servant au traitement de données personnelles et, le cas échéant, avec quel degré de détail. Ce point concerne spécialement les unités administratives qui n'utilisent plus des systèmes informatiques « monolithiques », mais des architectures plus modernes telles que les microservices, où les données traitées ne peuvent plus être cloisonnées dans des « silos » distincts. Pour la réglementation, ce n'est alors plus tant l'architecture informatique (technique) qui est au premier plan, mais bien plus l'« architecture de traitement des données » (notamment les finalités et la logique du traitement ainsi que le flux des données et l'accès à celles-ci). Il est important que, même lors de la dissolution de structures de données classiques, il soit à tout moment possible de reconnaître quelles données ont été traitées, par qui, et

[6] Le droit fondamental à l'autodétermination informationnelle selon l'art. 13, al. 2, Cst. garantit d'une manière générale, donc indépendamment de la sensibilité des données concernées, à toute personne le droit de pouvoir déterminer si et à quelles fins les informations la concernant peuvent être traitées par des tiers, qu'il s'agisse d'entités étatiques ou privées (ATF **146** I 11, consid. 3.1.1).

pour accomplir quelles tâches ou dans quel but. La « relation à la tâche » de tout traitement de données doit par conséquent également être établie dans les structures de type horizontal.

En résumé, les exigences en matière de densité normative ne sont généralement pas satisfaites lorsqu'une disposition prévoit simplement que le traitement des données doit permettre à l'organe fédéral compétent de remplir les tâches qui lui incombent de par la loi[7]. On peut être moins sévère dans les cas où les tâches d'un organe fédéral sont décrites de manière précise et que celui-ci ne procède pas à des traitements délicats ou complexes.

- **Exceptions à l'exigence de la base légale :** vu qu'il est difficilement possible de créer les dispositions nécessaires pour tous les cas de figure envisageables, la nLPD prévoit, à l'instar de la LPD, des exceptions à l'exigence de la base légale pour le traitement des données (art. 34, al. 4, nLPD[8] et art. 36, al. 2, nLPD[9]). Dans ces cas (énumérés exhaustivement), un traitement de données est admissible *sans base légale*, peu importe qu'il s'agisse d'un traitement « ordinaire » selon l'art. 34, al. 1, nLPD ou d'un traitement de données sensibles selon l'art. 34, al. 2, nLPD. Les exceptions admises dans la nLPD coïncident en majeure partie avec celles du droit en vigueur. Pour les modifications, nous renvoyons au message du Conseil fédéral du 15 septembre 2017 (► FF **2017** 6565, 6697 s.). Même si le nouveau libellé – à la différence de la disposition actuelle (art. 17, al. 2, LPD) – ne contient plus le terme « exceptionnellement », il n'y a pas de modification de la teneur. La règle reste la même : un traitement de données qui se caractérise par une certaine régularité ou durabilité doit pouvoir s'appuyer sur une base légale.

- **« Cas particuliers » :** tout comme l'actuelle loi, la nLPD contient plusieurs dispositions spéciales qui assouplissent les exigences concernant la base légale (pour les essais pilotes selon l'art. 35 nLPD ou pour le traitement de données à des fins ne se rapportant pas à des personnes selon l'art. 39 nLPD) ou qui autorisent directement des organes fédéraux à communiquer certaines données (communication facilitée des données de base selon l'art. 36, al. 4, nLPD). Une autre réglementation spéciale concerne la communication de données personnelles dans le cadre de l'information officielle du public par les organes fédéraux (art. 36, al. 3 et 5, nLPD). Ces dispositions particulières de la nLPD coïncident en majeure partie avec celles du droit en vigueur. Pour les modifications, nous renvoyons au message du Conseil fédéral du 15 septembre 2017 (► FF **2017** 6565, 6696 ss).

- **Rapport entre LPD et lois spéciales :** d'une manière générale, il y a égalité de rang entre les normes d'un même niveau. Il n'est dès lors pas exclu qu'une autre disposition légale

---

7 Les deux exemples des cantons de Thurgovie (ATF **146** II 11) et de Zurich (ATF **136** II 87) illustrent les exigences formulées par le Tribunal fédéral au sujet de la densité normative.

8 En vertu de l'art. 34, al. 4, nLPD, les organes fédéraux peuvent traiter des données personnelles sans disposer de base légale si : (a) le Conseil fédéral a autorisé le traitement, considérant que les droits des personnes concernées ne sont pas menacés ; (b) la personne concernée a consenti au traitement en l'espèce, selon l'art. 6, al. 6 et 7, nLPD, ou elle a rendu ses données personnelles accessibles à tout un chacun et ne s'est pas opposée expressément au traitement ; ou *nouveau* (c) le traitement est nécessaire pour protéger la vie ou l'intégrité corporelle de la personne concernée ou d'un tiers et il n'est pas possible d'obtenir le consentement de la personne concernée dans un délai raisonnable. *À la différence* de la disposition du droit actuel (art. 17, al. 2, let. a, LPD), aucune exception à l'exigence de la base légale n'est prévue pour le cas où l'accomplissement d'une tâche clairement définie dans une loi au sens formel exigerait absolument un traitement de données. Dans ce type de cas, les exigences concernant le niveau normatif sont toutefois réduites (voir art. 34, al. 3, nLPD ; ► point 2.2.1, let. a)/cc et b)/ee).

9 En vertu de l'art. 36, al. 2, nLPD, les organes fédéraux ont le droit, dans des cas individuels, de communiquer des données personnelles sans indiquer une base légale si : (a) la communication des données est indispensable au destinataire ou, *nouveau*, au responsable du traitement pour l'accomplissement d'une tâche légale ; (b) la personne concernée a consenti à la communication des données selon l'art. 6, al. 6 et 7, nLPD ; (c) la communication des données est nécessaire pour protéger la vie ou l'intégrité corporelle de la personne concernée ou d'un tiers et il n'est pas possible d'obtenir le consentement de la personne concernée dans un délai raisonnable (*nouveau*) ; (d) la personne concernée a rendu ses données accessibles à tout un chacun et ne s'est pas expressément opposée à la communication ; ou (e) le destinataire rend vraisemblable que la personne concernée ne refuse son consentement ou ne s'oppose à la communication que dans le but de l'empêcher de se prévaloir de prétentions juridiques ou de faire valoir d'autres intérêts légitimes.

formelle prime la nLPD à titre de loi spéciale[10]. Le législateur peut en conséquence s'écarter de certains principes de la nLPD dans les bases légales spécifiques de domaines particuliers, si les valeurs contenues dans une autre loi l'exigent. Le cadre défini par la Constitution et le droit international doit toutefois être respecté :

- La nLPD met en œuvre met en œuvre différents éléments de protection du *droit fondamental à l'autodétermination informationnelle garanti par l'art. 13, al. 2, Cst. et par l'art. 8 CEDH* (par ex. le droit d'accès, le droit à la rectification et à l'effacement). La restriction de ces garanties, concrétisées par la législation sur la protection des données, est soumise aux exigences de l'art. 36 Cst.

  Selon la jurisprudence du Tribunal fédéral, le **droit fondamental à l'autodétermination informationnelle** garantit d'une manière générale, indépendamment de la sensibilité des données concernées, à toute personne le droit de pouvoir déterminer si et à quelles fins les informations la concernant peuvent être traitées par des tiers, qu'il s'agisse d'entités étatiques ou privées[11]. La doctrine et la jurisprudence en déduisent différents droits spécifiques, dont au moins le droit de consulter ses propres données, le droit à rectifier des données personnelles erronées et le droit d'exiger la radiation de données personnelles traitées illicitement[12].

- Il faut en outre tenir compte du fait que la nLPD reprend des dispositions contraignantes pour la Suisse découlant du droit international et européen. Ainsi, les exigences de la *Convention 108+ du Conseil de l'Europe* et de la *directive de l'UE 2016/680 concernant la protection des données en matière pénale* limitent les dispositions des lois spéciales dérogeant à la nLPD.

- En dehors du champ d'application de la directive UE 2016/680 relative à la protection des données en matière pénale, la Suisse est considérée comme un État tiers par l'UE. En 2000, la Commission européenne a attesté que la Suisse offrait un niveau de protection des données adéquat. Cette *décision d'adéquation* signifie que des données personnelles provenant d'États membres de l'UE peuvent être communiquées à la Suisse sans exigences supplémentaires. La Commission européenne examine actuellement la décision d'adéquation de la Suisse. Des vérifications périodiques de la législation suisse en matière de protection des données sont prévues à l'avenir également. La Suisse ne pourra conserver sa décision d'adéquation que si elle assure un niveau de protection des données *adéquat* selon le règlement général de l'UE 2016/679 sur la protection des données. En l'occurrence, la Commission européenne évalue non seulement la protection des données dans la législation suisse en général, mais également dans le droit sectoriel. L'UE attache une importance particulière aux accès aux données par les autorités dans les domaines de la sécurité nationale et du droit pénal[13]. Au vu de cette situation, il convient de veiller à un niveau de protection des données adéquat dans les législations spécifiques également. Si la décision d'adéquation

[10] Voir par ex. ATF **142** II 268, consid. 6.3, ou l'arrêt du Tribunal administratif fédéral B-6547/2014 du 25 avril 2017, consid. 5.2.

[11] En lieu et place de nombreux autres, ATF **146** I 11, consid. 3.1.1. Voir aussi PASCAL MAHON, Le droit à l'intégrité numérique : réelle innovation ou simple évolution du droit ? Le point de vue du droit constitutionnel, in : Le droit à l'intégrité numérique, 2021, pp. 44-63 (en particulier pp. 47 s.).

[12] Voir ALEXANDRE FLÜCKIGER, L'autodétermination en matière de données personnelles : un droit (plus si) fondamental à l'ère digitale ou un nouveau droit de propriété ?, in : PJA 2013, pp. 837 ss (en particulier p. 852), avec d'autres indications. ALEXANDRE FLÜCKIGER déduit du droit fondamental de l'autodétermination informationnelle d'autres droits constitutionnels, notamment « le droit de spécifier le but de l'utilisation des données récoltées, le droit de s'opposer à leur traitement, le droit à la transparence de la collecte (caractère reconnaissable de celle-ci et devoir d'information), le droit de ne pas exporter ses données vers des pays moins protecteurs, le droit à la sécurité des données (protection en cas d'atteinte à l'intégrité des données suite à un traitement illicite ou contraire à sa volonté ainsi qu'en cas de brèche de sécurité [vol ou perte des données], comprenant en plus le droit d'être avisé en pareil cas), le droit à l'anonymat, en particulier celui d'aller et venir anonymement, le droit à l'oubli, le droit d'exiger un cadre et des moyens techniques permettant à chacun d'exercer effectivement des choix éclairés : architecture informatique conçue pour améliorer le pouvoir de contrôle (privacy enhancing technologies), protection intégrée de la vie privée (privacy by design), dépôts de données personnelles (personal data store), de même que le droit de disposer librement de ses données à sa mort (droit successoral numérique) ».

[13] Voir les Critères de référence pour l'adéquation du 28 novembre 2017 et du 6 février 2018 de l'ancien groupe de travail « Article 29 » sur la protection des données.

venait à être levée (partiellement ou complètement), l'échange de données transfrontières s'en trouverait considérablement compliqué. Voir à ce propos les art. 45 ss du règlement général de l'UE 2016/679 sur la protection des données.

Constat : les dérogations des lois spéciales à la nLPD (à titre de « norme minimale » en matière de protection des données) ne sont admises que pour de justes motifs et doivent être dûment motivées.

2.2 Ce qui *change* suite à la révision totale de la LPD

2.2.1 Exigences concernant le niveau normatif (une loi formelle est requise)

L'art. 34, al. 2 et 3 nLPD définit différentes conditions concernant le niveau normatif exigé pour des traitements de données sensibles par les organes fédéraux comportant des risques particulièrement importants. Ces exigences s'appliquent également à la communication des données (art. 36, al. 1, nLPD).

a) Traitement de données sensibles (art. 34, al. 2, let. a, nLPD)

aa) Inchangé : principe de la base légale au sens formel

En vertu de l'art. 34, al. 2, let. a, nLPD, le traitement de données sensibles doit être expressément prévu dans une loi au sens formel. Pour garantir la transparence à l'égard des personnes concernées, il convient de désigner dans la disposition légale les *catégories* de données sensibles, *selon l'art. 5, let. c, ch. 1 à 6, nLPD*, qui seront traitées. Conformément au principe de la proportionnalité, l'organe fédéral ne peut être habilité à traiter que les catégories de données dont il a besoin pour accomplir ses tâches. Si possible et nécessaire, des sous-catégories seront créées (exemple : il n'est pas permis de traiter toutes les données sur la santé, mais uniquement une sélection, telles que les données sur les cancers). Ces exigences correspondent au droit en vigueur. Il faut toutefois relever deux modifications :

- Le catalogue des données sensibles figurant à l'art. 5, let. c, nLPD a été élargi dans le cadre de la révision totale de la LPD (► voir ci-après let. bb).

- Il sera admissible, sous certaines conditions, de réglementer le traitement de données sensibles au niveau de l'ordonnance (► voir ci-après let. cc).

bb) Nouveau : élargissement du catalogue des données sensibles

La notion de données personnelles sensibles (données sensibles) est définie de manière exhaustive à l'art. 5, let. c, nLPD. Comme *jusqu'ici*, il s'agit de données sur les opinions ou les activités religieuses, philosophiques, politiques ou syndicales (ch. 1), sur la santé, la sphère intime ou l'origine raciale (ch. 2), sur des poursuites ou sanctions pénales et administratives (ch. 5) ainsi que les données sur des mesures d'aide sociale (ch. 6). Viennent *s'ajouter* les catégories suivantes de données sensibles :

- **Données sur l'origine ethnique** (art. 5, let. c, ch. 2, nLPD) : dans la jurisprudence du Tribunal fédéral relative à l'art. 261bis CP, une ethnie est définie comme étant un segment de la population qui se considère lui-même comme un groupe distinct et que le reste de la population perçoit également comme groupe. Une ethnie doit avoir une histoire commune

ainsi qu'un système commun et cohérent de valeurs et de normes comportementales (traditions, coutumes, usages, langue, etc.), ces caractéristiques devant être utilisées pour délimiter le groupe[14].

Exemples : Albanais du Kosovo, Arabes, Palestiniens ou gens du voyage[15].

- **Données génétiques** (art. 5, let. c, ch. 3, nLPD) : selon le message du Conseil fédéral du 15 septembre 2017, les données génétiques « sont les informations relatives au patrimoine génétique d'une personne obtenues par une analyse génétique » (► FF **2017** 6565, 6640)[16]. Cette définition correspond à l'art. 3, let. l, de la loi fédérale sur l'analyse génétique humaine.

  Exemple : profil ADN.

- **Données biométriques identifiant une personne physique de manière univoque** (art. 5, let. c, ch. 4, nLPD) : les données biométriques au sens de l'art. 5, let. c, ch. 4, nLPD sont les données personnelles obtenues à l'aide d'un *procédé technique spécifique* et qui se rapportent aux *caractéristiques physiques, physiologiques ou comportementales* d'une personne physique et permettent ou confirment son *identification unique* (► FF **2017** 6565, 6641). À la différence des données génétiques, le procédé technique utilisé pour les données biométriques et permettant l'*identification univoque* de la personne concernée fait partie intégrante de la qualification de données sensibles. Sans cette restriction, des photographies ou des enregistrements sonores ordinaires seraient également considérés comme des données sensibles.

  Exemples : photographies du visage traitées avec un logiciel de reconnaissance faciale, empreintes digitales, images de l'iris et de la rétine.

Les notions de « données génétiques » et de « données biométriques » permettant une identification univoque d'une personne physique sont très vastes. Il est dès lors essentiel de préciser dans la base légale au sens formel *quelles* données génétiques ou biométriques seront traitées. Il faut faire preuve de retenue en ce qui concerne les normes de délégation.

À titre d'exemple d'une norme de délégation, voir l'art. 2*b*, al. 4, du projet de loi du 4 décembre 2020 sur les profils ADN[17] concernant le phénotypage : « Le Conseil fédéral peut définir des caractéristiques morphologiques apparentes supplémentaires en fonction des progrès techniques et à condition que la fiabilité pratique des nouvelles méthodes visant à déterminer ces caractéristiques soit établie ».

L'extension du catalogue des données sensibles transpose dans le droit suisse les exigences énoncées à l'art. 6, al. 1, de la Convention 108+ du Conseil de l'Europe ainsi que les art. 3, ch. 12 et 13, et 10 de la directive de l'UE 2016/680 relative à la protection des données dans le domaine pénal (développement de l'acquis de Schengen). La législation suisse sur la protection des données se rapproche aussi du règlement général de l'UE 2016/679 sur la protection des données (art. 4, ch. 13 et 14, ainsi qu'art. 9). Les réglementations européennes doivent par conséquent être prises en compte lors de l'interprétation de l'art. 5, let. c, nLPD.

cc) Nouveau : réduction des exigences relatives au niveau normatif à certaines conditions

[14] ATF **143** IV 193, consid. 2.3.

[15] FABIENNE ZANNOL, Die Anwendung der Strafnorm gegen Rassendiskriminierung (étude sur mandat de la CFR), Berne 2007.

[16] La restriction demandée par le Conseil national pour la définition du terme « données génétiques » à l'art. 5, let. c, ch. 3, nLPD, à savoir qu'elles ne seraient sensibles que si « elles identifient clairement une personne physique », a été rejetée par le Conseil des États (= version du Conseil fédéral). La petite Chambre s'est imposée lors de l'élimination des divergences. Pour balayer les éventuels malentendus, la cheffe du DFJP a précisé au Conseil national que l'art. 5, let. c, ch. 3, nLPD n'incluait pas toutes les données génétiques, mais uniquement les données *personnelles* génétiques (= données qui se rapportent à une personne physique identifiée ou identifiable ; art. 5, let. a, nLPD). En d'autres termes : les données génétiques ne sont sensibles que si elles comprennent des informations permettant d'identifier assez aisément une personne concernée. Si tel n'est pas le cas (par ex. données anonymisées), les données génétiques n'entrent pas dans le champ d'application de la nLPD (voir Bulletin officiel **2019** N 1787).

[17] FF **2021** 45.

L'art. 34, al. 3, nLPD dispose désormais[18] qu'il suffit d'une base légale prévue dans une loi au sens matériel pour autoriser le traitement de données sensibles, si deux conditions sont remplies (cumulativement) :

- **Le traitement est indispensable à l'accomplissement d'une tâche définie dans une loi au sens formel :** la tâche requérant le traitement des données personnelles doit être prévue dans une loi au sens formel et son étendue doit y être clairement définie. C'est la condition pour assurer la transparence nécessaire à l'égard de la personne concernée. Une tâche qui serait dérivée implicitement de la loi n'est pas suffisante pour justifier un traitement. En outre, le traitement doit être indispensable à l'accomplissement de la tâche. Cette condition n'est remplie que s'il est impossible d'accomplir la tâche sans traiter les données visées. Il ne suffit pas que l'accomplissement de la tâche s'en trouve amélioré[19].

- **La finalité du traitement ne présente pas de risques particuliers pour les droits fondamentaux de la personne concernée :** il s'agit surtout de la protection de la sphère privée, selon l'art. 13 Cst. Contrairement à sa formulation (trop) restrictive, l'art. 13, al. 2, Cst. assure, selon la doctrine dominante et la jurisprudence du Tribunal fédéral, non seulement la protection contre l'utilisation abusive des données personnelles, mais donne également un droit très complet à l'autodétermination informationnelle. Cela signifie que toute personne peut décider elle-même si les informations la concernant peuvent être traitées et à quelles fins (► voir point 2.1)[20]. Le droit à la liberté personnelle inscrit à l'art. 10, al. 2, Cst. offre une garantie constitutionnelle fondamentale pour la protection de la personnalité (notamment la protection **des libertés élémentaires dont l'exercice est indispensable à l'épanouissement de la personnalité humaine).** D'autres droits fondamentaux, à l'instar de la liberté économique (art. 27 Cst.), doivent également être respectés. Pour les cas dans lesquels le but du traitement constitue une restriction grave aux droits fondamentaux de la personne concernée, ► voir point 2.2.1, let. c)/bb. Il convient en outre de souligner que les risques pour les droits fondamentaux de la personne concernée ne sont pas liés uniquement à la finalité du traitement, mais peuvent découler aussi du mode de traitement ; voir à ce propos l'art. 34, al. 2, let. c, nLPD ainsi que ► point 2.2.1, let. c)/cc.

b) Profilage (art. 34, al. 2, let. b, nLPD)

aa) Situation initiale : du profil de la personnalité au profilage

Les progrès techniques ont fait apparaître de nouvelles méthodes de traitement des données. Ils ont notamment permis d'enregistrer de grandes quantités de données, de les relier entre elles et de les analyser (« Big Data »). De cette pléthore de données, qui, prises individuellement, peuvent ne pas être très révélatrices, il est possible de tirer de nouvelles informations sur les personnes à l'aide de procédés mathématiques et statistiques. La révision totale de la LPD tient compte de cette évolution de la technologie, notamment en remplaçant le terme « profil de la personnalité » (art. 3, let. d, LPD) par « profilage » (art. 5, let. f et g, nLPD). Même si de prime abord ces deux termes paraissent très similaires, ils ne sont pas identiques. Un **profil de la personnalité** est le *résultat d'une procédure de traitement* (= compilation de données fournissant une image sur des aspects [partiels] importants d'une personne physique) ; le **profilage**, lui, est un *type ou une méthode de traitement des données* (= évaluation automatisée de certains aspects d'une personne physique).

---

[18] En vertu de l'actuel art. 17, al. 2, let. a, LPD, il est permis de traiter des données sensibles *sans base légale*, si exceptionnellement l'accomplissement d'une tâche clairement définie dans une loi au sens formel l'exige absolument. Le traitement de données ne peut toutefois s'appuyer sur cette dérogation que dans le cas particulier (voir CLAUDIA MUND, Stämpflis Handkommentar zum Datenschutzgesetz, Berne 2015 [« SHK DSG »], N 15 ad art. 17 LPD).

[19] Voir l'ATF **147** II 227, indiquant que « indispensable » signifie qu'une tâche légale ne peut être remplie qu'à l'aide des données concernées et qu'il s'agit de l'unique possibilité pour son accomplissement (consid. 5.4).

[20] ATF **140** I 2, consid. 9.1.

Comme c'est le cas aujourd'hui pour le traitement de profils de la personnalité, la nLPD prévoit des effets juridiques qualifiés pour le profilage (ou, les traitements de données par des personnes privées pour le profilage à risque élevé). Ainsi, le profilage par des organes fédéraux requiert une autorisation reposant sur une base légale formelle (► voir ci-dessous let. dd). Le profilage peut entraîner des risques particuliers pour les droits fondamentaux de la personne concernée. En effet, les processus de profilage sont souvent peu transparents, surtout si le profilage est établi à l'aide d'algorithmes. Les personnes concernées ne savent pas selon quelle logique leurs données sont traitées ni quelles conséquences ce traitement peut avoir pour elles. Le profilage permet d'analyser des personnalités, de les classer dans des catégories et de les évaluer. Non seulement des clichés existants peuvent ainsi être consolidés, mais il est possible d'aboutir à des prévisions erronées et à des discriminations.

bb) La notion de « profilage » (art. 5, let. f, nLPD)

Le Parlement s'est écarté de la définition légale du profilage proposée dans le projet du Conseil fédéral et s'est inspiré du **libellé de la réglementation de l'UE en matière de protection des données** (art. 3, ch. 4, de la directive de l'UE 2016/680 relative à la protection des données en matière pénale ; art. 4, ch. 4, du règlement général de l'UE 2016/679)[21]. Le Conseil fédéral avait initialement choisi sa propre description du profilage, sans volonté toutefois de s'écarter de la teneur du droit européen (► FF **2017** 6565, 6641 s.). Cet historique révèle que les prescriptions européennes jouent un rôle important pour l'interprétation du terme « profilage ».

L'art. 5, let. f, nLPD définit le **profilage** comme « 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 ». Plus précisément :

- Le **traitement des données**, en particulier la procédure d'évaluation[22], se fait de manière **automatisée**. À la différence de la notion de décision individuelle automatisée (► voir point 2.2.1, let. c)/cc), le traitement de données pour le profilage n'est pas forcément *entièrement automatisé*. L'intervention d'une personne n'exclut pas le profilage, tant que le traitement des données se fait *essentiellement de façon automatisée*[23].

- L'**objectif du traitement des données** consiste à **évaluer** des aspects personnels d'une personne physique. L'évaluation peut consister en une *analyse* de traits de la personnalité, mais elle peut également servir à faire des *prévisions* sur les futurs comportements ou caractéristiques d'une personne. À titre d'illustration, la définition légale à l'art. 5, let. f, nLPD mentionne quelques exemples (analyse ou prédiction des éléments concernant le rendement au travail, situation économique, santé, préférences personnelles, localisation ou déplacements).

---

[21] Voir à ce propos l'intervention du rapporteur de la CIP-N MATTHIAS JAUSLIN au Conseil national le 24 septembre 2019 : BO **2019** N 1790.

[22] Voir l'exemple de SIMON ROTH, Das Profiling im neuen Datenschutzrecht, in : RSDA 2021 34–39, p. 35 : Si un détective privé observe une personne afin de vérifier son état de santé en rapport avec des allégations liées aux assurances sociales, et qu'il utilise un appareil photo ou une caméra pour ce faire, il n'y a pas encore profilage. En effet, l'appréciation, qui consiste à dire si la personne observée présente bien les problèmes de santé déclarés, se fait par analyse manuelle des photos ou des enregistrements vidéo et non pas de manière automatisée. L'appareil photo ou la caméra ne tire aucune conclusion concernant l'état de santé de la personne concernée.

[23] Voir les « Lignes directrices relatives à la prise de décision individuelle automatisée et au profilage aux fins du règlement (UE) 2016/679 » du 6 février 2018 de l'ancien groupe de travail « Article 29 » sur la protection des données, p. 7. Dans l'intervalle, ces lignes directrices ont été reprises par le Comité européen de protection des données (CEPD). Voir également DAVID VASELLA, Profiling nach der DSGVO und dem E-DSG bei Banken, in : SUSAN EMMENEGGER (éd.), Banken und Datenschutz, Bâle 2019, p. 197. Dans le message du Conseil fédéral du 15 septembre 2017, il est précisé que le terme profilage se rapporte à une évaluation entièrement automatisée. Cette affirmation est trop absolue au regard de l'adaptation de la définition légale par le Parlement (harmonisation avec le droit de l'UE en matière de protection des données) et de l'interprétation du terme « profilage » dans les actes législatifs européens.

Le choix du terme « évaluer » indique que le profilage consiste en une sorte d'appréciation ou d'estimation concernant une personne. En clair, le profilage vise à analyser certaines caractéristiques d'une personne afin de déterminer si elle est qualifiée ou non pour exercer certaines activités. Il se fonde sur une hypothèse de base, à savoir qu'une personne se comportera de manière identique ou similaire à ce qu'elle a fait par le passé ou qu'une personne présentant un profil donné se comporte comme d'autres individus ayant un profil identique ou similaire. Il s'agit par conséquent de probabilités, qui ne correspondent pas obligatoirement à la réalité[24]. Le profilage n'est donc jamais un constat objectif de faits. Une simple répartition de personnes selon des caractéristiques connues telles que l'âge, le sexe ou la taille ne constitue pas forcément un profilage. En l'occurrence, c'est le motif de cette catégorisation qui est déterminant. Ainsi, une personne peut traiter les données de sa clientèle à des fins statistiques, les classer par âge ou par sexe afin d'avoir une vue d'ensemble, sans faire de prévisions ou tirer de conclusions concernant des individus. Dans un tel cas, la répartition n'a pas pour but l'évaluation de caractéristiques individuelles. Il ne s'agit donc pas d'un profilage[25]. La simple compilation de données clés, telles que nom, date de naissance et sexe (à des fins d'identification), ne constitue pas non plus un profilage, vu qu'aucune évaluation des caractéristiques personnelles n'a lieu[26].

Exemples[27] (sans distinction entre profilage « ordinaire » ou profilage « à risque élevé » ; ► voir ci-après let. cc) :

- *Évaluation de la situation économique ou de la solvabilité :* le score de crédit (« credit scoring ») est une méthode mathématique et statistique permettant d'évaluer la solvabilité d'une personne (solvabilité et volonté de payer). Cette analyse inclut des informations concernant des mises aux poursuites, des actes de défaut de biens, un blocage de comptes bancaires et de cartes de crédit en raison de retards de paiement, des demandes de crédits, des procédures de paiement ou de recouvrement ou des expériences tirées d'anciennes relations d'affaires. La personne concernée se voit attribuer une notation de crédit (score), qui sera utilisée par exemple pour décider de l'octroi d'un prêt ou définir les modalités de paiement (achat contre facture). Si l'attribution du score se fait de manière automatisée (et non manuellement), il s'agit d'un profilage.
- *Évaluation de la santé :* si un dispositif de suivi de l'activité physique compte uniquement les pas, il n'y a en principe pas d'évaluation de la santé de la personne et donc pas de profilage. Si le comptage des pas est en revanche combiné avec d'autres données, par exemple la taille, le poids, le sexe, les habitudes alimentaires, le rythme de sommeil ou les données GPS, des analyses de l'état de santé sont possibles. Une telle analyse (automatisée) de la santé constitue un profilage.
- *Évaluation des préférences personnelles :* il y a lieu de soupçonner un profilage lorsque les personnes concernées sont classées dans différentes catégories, par exemple sur la base de diverses méthodes de traçage des utilisateurs sur Internet, à l'aide notamment des cookies indiquant les pages Internet visitées, des likes sur les réseaux sociaux ou des applications utilisées sur un smartphone, et que ces catégories correspondent à des schémas comportementaux (par ex. « fait beaucoup de sport », « est végétarien », « se concentre sur le travail » ou « est introverti/extroverti »). Ce type d'analyse est ensuite utilisé pour des publicités personnalisées notamment.
- *Évaluation du comportement :* dans le secteur public, on pourrait être en présence d'un profilage lorsqu'une autorité policière évalue des données personnelles de façon automatisée afin d'estimer le niveau de dangerosité d'une personne.
- *Évaluation du comportement :* la FINMA obtient de très nombreuses données dans le cadre de sa surveillance des marchés financiers, desquelles il est possible de déduire, par profilage, un éventuel comportement fautif sous l'angle du droit de la surveillance. En particulier dans le cadre de la surveillance des marchés (par ex.

[24] OLIVIER HEUBERGER, Profiling im Persönlichkeits- und Datenschutzrecht der Schweiz, thèse, Lucerne 2020, ch. 59.

[25] Voir les « Lignes directrices relatives à la prise de décision individuelle automatisée et au profilage aux fins du règlement (UE) 2016/679 » du 6 février 2018 de l'ancien groupe de travail « article 29 » sur protection des données, p. 7 ; DAVID ROSENTHAL, La nouvelle loi sur la protection des données, in : Jusletter du 16 novembre 2020, ch. 24; DAVID VASELLA, op. cit., pp. 193 s.

[26] OLIVIER HEUBERGER, op. cit., ch. 147.

[27] Les trois premiers exemples sont tirés d'OLIVIER HEUBERGER, op. cit., ch. 157 ss.

pour une clarification sur un possible délit d'initié ou une manipulation de marché), la FINMA procède à des analyses automatisées de données relatives aux échanges commerciaux ou aux transactions, et qui sont en lien avec des personnes (► voir le message du Conseil fédéral du 15 septembre 2017, FF **2017** 6565, 6765 à propos du nouvel art. 23, al. 3, LFINMA).

cc) La notion de « profilage à risque élevé » (art. 5, let. g, nLPD)

La notion de profilage à risque élevé a été introduite durant les **délibérations parlementaires**. Le Parlement a estimé que le projet du Conseil fédéral était trop strict en ce qui concerne le profilage, surtout pour le traitement de données par des personnes privées. L'exécutif avait en effet classé le profilage *en soi* comme présentant un risque et n'avait pas tenu compte du fait que le profilage pouvait également consister en des procédures inoffensives. D'où le choix du Parlement de prévoir une approche fondée sur le risque. Dès lors, le profilage issu du traitement de données par des responsables du traitement privés ne doit avoir des conséquences juridiques qualifiées que s'il est « à risque élevé ». Pour les organes fédéraux en revanche, la distinction entre profilage « ordinaire » et « à risque élevé » n'a que peu de conséquences (► voir ci-après let. dd).

Le Conseil national et le Conseil des États n'ont pu s'accorder sur la **définition légale du profilage à risque élevé** que lors de la Conférence de conciliation[28]. L'art. 5, let. g, nLPD précise qu'il s'agit de tout « profilage entraînant 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 ». Explications :

- La description du risque élevé à l'art. 5, let. g, nLPD correspond à l'**actuelle notion de « profil de la personnalité »** selon l'art. 3, let. d, LPD. Seule l'expression « assemblage de données » est remplacée par « appariement de données » afin de mieux tenir compte sur le plan linguistique des nouvelles possibilités technologiques. Il en découle que la jurisprudence relative au profil de la personnalité (en particulier l'arrêt principal du Tribunal administratif fédéral dans l'affaire Moneyhouse[29]) reste déterminante.

- Pour simplifier, il y a profilage à risque élevé au sens de l'art. 5, let. g, nLPD lorsque son **résultat** est un profil de la personnalité au sens de la LPD en vigueur. Il s'agit par conséquent d'une combinaison entre méthode de traitement des données (profilage) et résultat du traitement des données (profil de la personnalité).

- Cette définition légale tient compte du fait qu'un grand nombre de données (même si elles ne sont pas particulièrement sensibles) peuvent être appariées et donner une **image de la personne concernée** qui, elle, constitue un risque élevé pour les droits de la personnalité et les droits fondamentaux. La personne concernée n'a souvent aucun moyen d'influer sur cette image et ne peut contrôler ni sa justesse ni son utilisation. Elle se trouve par conséquent limitée dans sa liberté de se représenter comme elle le tient pour juste. Si des données personnelles sont collectées sur une longue période (« profil sur la durée »), elles débouchent plus aisément sur un profil de la personnalité ou un profilage à risque élevé que s'il ne s'agit que d'un relevé momentané[30].

Exemples :

– le GPS intégré dans un smartphone permet en principe de localiser l'appareil à quelques mètres près. Le traitement des *données de mouvement d'un smartphone* peut être automatisé en vue de tirer des conclusions sur son propriétaire. Si ces données ne sont analysées que sur une courte durée et pour un endroit précis (par

[28] Séances du Conseil national (BO **2020** N 1816 ss) et du Conseil des États du 24 septembre 2020 (BO **2020** E 1024 ss).

[29] Arrêt du Tribunal administratif fédéral A-4232/2015 dans l'affaire PFPDT contre Moneyhouse SA du 18 avril 2017.

[30] Voir SIMON ROTH, op. cit., p. 36 avec d'autres indications.

ex. passage dans une gare), il n'y a généralement qu'un *« profilage ordinaire »*. Par contre, si les données de mouvement sont enregistrées sur une période plus longue, dans un rayon géographique plus étendu, elles permettent de tirer des conclusions sur toute une série de domaines de la vie d'une personne. C'est vrai pour le lieu de travail, les conditions de logement, les habitudes alimentaires, les relations personnelles, les éventuelles visites chez un médecin ou les habitudes de consommation. Il en résulte une image de la personne (profil de la personnalité), qui mérite d'être spécialement protégée. Dans un tel cas, il y aurait lieu de supposer un *profilage à risque élevé*.

– Un profilage pour *vérifier la solvabilité* qui ne se fonde pas uniquement sur les données relatives à la situation économique et la capacité de paiement de la personne concernée, mais inclut également des données sur d'autres aspects de sa personnalité (tels que les conditions de logement et la situation de vie) doit être qualifié de *profilage à risque élevé*[31].

Dans la pratique, le profilage réalisé par des organes fédéraux peut aboutir à des atteintes graves aux droits fondamentaux des personnes concernées pour d'autres motifs (c.-à-d. sans que son résultat soit un profil de la personnalité). Songeons par exemple au profilage de mineurs ou d'autres personnes vulnérables, ou encore à celui dont le but est de refuser d'importantes prestations. Il convient de tenir compte de ces risques lors de l'élaboration des bases légales selon les art. 34 ss nLPD ou encore dans l'analyse d'impact relative à la protection des données personnelles selon l'art. 22 nLPD (► point 4.3), ces dispositions ne faisant pas référence à l'existence d'un profilage à risque élevé selon l'art. 5, let. g, nLPD.

dd) Principe : loi au sens formel

L'art. 34, al. 2, let. b, nLPD prévoit que les organes fédéraux doivent en règle générale être habilités, par une **base légale au sens formel**, à faire des profilages. Cette disposition remplace l'actuel art. 17, al. 2, LPD qui dispose que les organes fédéraux ne peuvent traiter des profils de la personnalité que si une loi au sens formel le prévoit expressément. Cette exigence s'applique non seulement au profilage à risque élevé, mais également au profilage « ordinaire ». Fixer la base légale au niveau de l'ordonnance n'entre en ligne de compte que dans les conditions énoncées à l'art. 34, al. 3, nLPD (► voir ci-après let. ee).

La base légale formelle pour le profilage doit présenter une **précision suffisante**. Ainsi, elle doit prévoir explicitement le profilage ou le décrire conformément à la définition fixée à l'art. 5, let. f, nLPD. Il en va de même du profilage à risque élevé selon l'art. 5, let. g, nLPD. En vertu du principe de proportionnalité, les organes fédéraux ne doivent être habilités à procéder à un profilage (à risque élevé) que s'il est indispensable à l'accomplissement de leurs tâches. Il convient dans tous les cas d'envisager également d'autres méthodes de traitement des données. L'évaluation de la proportionnalité doit notamment répondre à la question de savoir si, pour une même efficacité, d'autres options de traitement permettraient de mieux protéger la personne concernée. En outre, la base légale doit définir au moins la finalité du profilage et les catégories de données sensibles selon l'art. 5, let. c, ch. 1-6, nLPD qu'il est prévu d'utiliser pour le profilage. La personne concernée doit pouvoir reconnaître quels traits de sa personnalité seront évalués à travers le profilage. Il convient de déterminer dans le cas particulier quels autres points doivent éventuellement être précisés dans la base légale (par ex. quelles données personnelles « ordinaires » sont incluses dans le profilage). Les précisions doivent porter sur les paramètres du profilage qui sont particulièrement importants eu égard à l'atteinte au droit à l'autodétermination informationnelle. Finalement, il est essentiel que les organes fédéraux réduisent au strict minimum le risque d'erreur et de discrimination dans le contexte du

[31] Pour évaluer ces faits en vertu du droit en vigueur ou eu égard à la notion de profil de la personnalité, voir l'arrêt du Tribunal administratif fédéral dans l'affaire A-4232/2015, PFPDT contre Moneyhouse SA du 18 avril 2017.

profilage, en recourant à des méthodes mathématiques ou statistiques et en appliquant des mesures techniques et organisationnelles appropriées.

Enfin se pose la question de savoir s'il faut également créer des bases légales spécifiques pour l'utilisation de **données tirées d'un profilage**. Celles-ci ne constituent pas toujours des données sensibles. Il peut en effet s'agir d'informations personnelles « ordinaires » (par ex. indiquant qu'une personne est jugée non solvable). Cette question devrait être étudiée pour chaque projet législatif et appréciée en fonction du contexte concret.

ee) Réduction des exigences relatives au niveau normatif à certaines conditions

Comme pour le traitement de données sensibles, une base légale dans une loi au sens matériel (art. 34, al. 3, nLPD) suffit pour le profilage, si ces deux conditions sont remplies (cumulativement) :

- le profilage **est indispensable à l'accomplissement d'une tâche définie dans une loi au sens formel** ;
- la **finalité du profilage** ne présente **pas de risques particuliers** pour les droits fondamentaux de la personne concernée.

Voir les explications au ► point 2.2.1, let. a)/cc.

c) Atteinte grave aux droits fondamentaux de la personne concernée (art. 34, al. 2, let. c, nLPD)

aa) Exigence d'une base légale au sens formel

L'art. 34, al. 2, let. c, nLPD prévoit désormais expressément ce qui est déjà valable en vertu de l'art. 36, al. 1, Cst. : peu importe qu'il s'agisse du traitement de données sensibles ou d'un profilage, il faut une base dans une loi au sens formel lorsque la **finalité du traitement** (► ci-après let. bb) ou le **mode de traitement** (► ci-après let. cc) peuvent aboutir à une **atteinte grave aux droits fondamentaux** de la personne concernée (► pour les droits fondamentaux pertinents, voir point 2.2.1, let. a)/cc). Un allégement des exigences concernant le niveau normatif selon l'art. 34, al. 3, nLPD n'est pas admis dans ces cas. Outre la sévérité de l'atteinte aux droits fondamentaux de la personne concernée, il y a d'autres critères dont il faut tenir compte comme la taille du groupe cible, l'importance politique, l'acceptation au sein de la population, l'écart par rapport aux réglementations en vigueur ou la dimension temporelle des conséquences du traitement des données.

bb) Atteinte grave aux droits fondamentaux en raison de la finalité du traitement (premier cas de figure de l'art. 34, al. 2, let. c, nLPD)

L'atteinte grave aux droits fondamentaux de la personne concernée peut découler de la **finalité du traitement des données**. Le message du Conseil fédéral du 15 septembre 2017 donne un exemple, en indiquant que les organes fédéraux doivent traiter des données personnelles dans certains domaines, notamment pour apprécier la dangerosité d'une personne, son potentiel à exercer une fonction, son aptitude à accomplir une obligation légale ou encore son mode de vie. Selon la finalité poursuivie par l'organe fédéral, un tel traitement de données peut porter gravement atteinte aux droits fondamentaux de la personne concernée, indépendamment de la nature des données traitées ; dans un tel cas, il est impératif qu'il repose sur une loi au sens formel (► FF **2017** 6565, 6695 s.). Dans cet exemple consistant à évaluer certaines caractéristiques d'une personne, il convient de tenir compte du fait que, si le degré

d'automatisation du traitement des données est élevé, il pourrait également s'agir d'un profilage au sens de l'art. 5, let. f, nLPD (► point 2.2.1, let. b).

cc) Atteinte grave aux droits fondamentaux en raison du mode de traitement (deuxième cas de figure de l'art. 34, al. 2, let. c, nLPD)

L'atteinte grave aux droits fondamentaux de la personne concernée peut découler du **mode de traitement des données.** Cela peut être le cas si la manière de collecter les données (surtout si elle se fait à l'insu de la personne concernée ou au moyen de caméras de surveillance) entraîne une atteinte dont la gravité exige une base légale au sens formel. Pour les nouvelles technologies (par ex. procédés biométriques tels que la reconnaissance faciale), il faut en règle générale des bases légales formelles et claires[32].

Ci-après, nous nous attachons surtout au **recours à l'intelligence artificielle**[33] **au sein de l'administration**. L'administration peut se servir de l'intelligence artificielle dans différents domaines et à des degrés plus ou moins poussés. Les possibilités d'utilisation vont du simple *soutien sur le plan interne, avec aucune ou très peu de répercussions extérieures* (par ex. applications qui distribuent automatiquement les tâches entre les membres du personnel, qui traduisent des documents ou qui rédigent des procès-verbaux de réunion) aux *systèmes qui prennent eux-mêmes les décisions* (automatisation complète), en passant par des *systèmes qui soutiennent l'administration dans ses prises de décision* (automatisation partielle). Nous nous intéressons ci-après aux deux derniers cas de figure. La nLPD contient différentes dispositions relatives aux décisions individuelles automatisées (automatisation complète ; cas 1). Dans la pratique actuelle, c'est toutefois l'utilisation de l'intelligence artificielle pour soutenir la prise de décision qui revêt la plus grande importance (automatisation partielle ; cas 2). Le potentiel de l'intelligence artificielle réside en premier lieu dans la gestion d'une grande masse de données, à savoir là où l'administration doit rendre des décisions dans un grand nombre de cas similaires (par ex. procédures relatives à l'imposition fiscale ou aux assurances sociales)[34].

Remarque : un groupe de travail interdépartemental institué par la Confédération et placé sous la direction du Secrétariat d'État à la formation, à la recherche et à l'innovation (SEFRI), s'est penché sur le recours à l'intelligence artificielle. Ces travaux ont débouché notamment sur le document « 'Intelligence artificielle' – lignes directrices pour la Confédération », que le Conseil fédéral a adopté le 25 novembre 2020[35]. Un débat approfondi sur les défis d'ordre juridique et éthique en rapport avec l'intelligence artificielle se trouve en outre dans l'étude « Einsatz Künstlicher Intelligenz in der Verwaltung » du 28 février 2021 mandatée par le canton de Zurich. C'est de cette étude que sont tirés les exemples ci-après illustrant l'application de l'intelligence artificielle dans l'administration (cantonale surtout).

Exemples[36] :

---

[32] Voir DAVID ROSENTHAL/YVONNE JÖHRI, Handkommentar zum Datenschutzgesetz, Zurich 2008 (« Handkommentar DSG »), N 26 ss.ad art. 17 LPD ; CLAUDIA MUND, SHK DSG, N 9 ad art. 17 LPD.

[33] Il n'existe pas encore de définition universelle de l'intelligence artificielle. Pour la terminologie et le mode de fonctionnement, voir NADJA BRAUN BINDER/MATTHIAS SPIELKAMP/CATHERINE EGLI, in : Staatskanzlei Kanton Zürich (éd.), Einsatz Künstlicher Intelligenz in der Verwaltung, 28 février 2021, p. 10. Dans le rapport « Défis de l'intelligence artificielle » du groupe de travail interdépartemental « Intelligence artificielle » du 13 décembre 2019, la notion d'intelligence artificielle (IA) n'est pas définie de manière abstraite ; elle est bien plus caractérisée à travers différents éléments structurels. Selon ce rapport, les systèmes d'IA sont capables (1) d'analyser des données sous une forme que ne permettraient pas d'autres technologies dans leur état actuel en termes de complexité et de volume, notamment avec des algorithmes identifiant de manière autonome, par apprentissage, des caractéristiques statistiques pertinentes dans les données ; (2) de faire des prédictions servant de base essentielle à des décisions (notamment décisions automatisées) ; (3) de reproduire des aptitudes associées à la cognition et à l'intelligence humaines ; (4) d'agir de manière largement autonome sur cette base.

[34] Pour cette question en général, voir JESSICA WULF/CATHERINE EGLI, in : Staatskanzlei Kanton Zürich (éd.), Einsatz Künstlicher Intelligenz in der Verwaltung, 28 février 2021, pp. 23 s.

[35] Voir le site Internet du SEFRI, consultable à l'adresse <https://www.sbfi.admin.ch/sbfi/fr/home/politique-fri/fri-2021-2024/themes-transversaux/numerisation-fri/intelligence-artificielle.html>.

[36] Les exemples sont tirés de NADJA BRAUN BINDER/CATHERINE EGLI/LAURENT FREIBURGHAUS/ELIANE KUNZ/NINA LAUKENMANN/LILIANE OBRECHT, in : Staatskanzlei Kanton Zürich (éd.), Einsatz Künstlicher Intelligenz in der Verwaltung, 28 février 2021, pp. 23 s.

- *Procédures fiscales :* actuellement, plusieurs cantons étudient les possibilités d'utilisation de l'intelligence artificielle pour les procédures fiscales. Aujourd'hui déjà, les déclarations d'impôt numériques sont traitées de manière partiellement automatisée dans la plupart des cantons, à l'aide de programmes de taxation. À l'avenir, l'intelligence artificielle soutiendra davantage encore les administrations fiscales. En l'occurrence, c'est principalement la taxation entièrement automatisée qui est favorisée. Accessoirement, l'intelligence artificielle pourrait cependant aussi être utilisée à titre de soutien pour les décisions ; elle pourrait par exemple aider les personnes contrôlant les déclarations, en leur indiquant les domaines où se produisent des erreurs, ou assurer la mise en correspondance automatique entre la déclaration d'impôt et les documents remis.
- *Procédure en matière d'assurances sociales :* il y a encore peu de technologies basées sur l'intelligence artificielle dans le domaine du droit social en Suisse. Le canton de Genève surtout souhaite utiliser l'intelligence artificielle pour lutter contre la fraude dans les assurances sociales. Elle doit permettre notamment de repérer les prestations sociales perçues injustement (par ex. mise au point d'algorithmes pour des systèmes de mise en garde et de rappel, pour l'exécution de contrôles de cohérence et d'analyses croisées des fluctuations du revenu et de la fortune).
- *« Prévision policière » se rapportant à des lieux :* les polices cantonales d'Argovie et de Bâle-Campagne ainsi que la police municipale zurichoise utilisent un logiciel développé en Allemagne, PRECOBS, pour lutter contre les cambriolages. L'application à d'autres types de délits est à l'étude. PRECOBS repose sur la théorie que les cambriolages (professionnels) sont fréquemment commis en série, de façon concentrée sur les plans temporel et géographique. Le logiciel fait des prévisions sur les probabilités accrues d'effractions dans certaines zones, à certains moments.
- *« Prévision policière » se rapportant à des personnes :* quelques cantons (dont Lucerne et Saint-Gall) recourent à l'outil d'analyse DyRiAS-Intimpartner, qui analyse le risque potentiel qu'une personne de sexe masculin commette des actes de violence contre sa partenaire actuelle ou d'anciennes compagnes. Il s'est toutefois avéré que DyRiAS surestime le risque.
- La *reconnaissance des véhicules et la surveillance du trafic automatisées*[37] saisissent les plaques d'immatriculation des véhicules à l'aide d'une caméra et déterminent l'identité de son détenteur ainsi que l'heure et le lieu du passage, la direction et les autres occupants du véhicule. Ces données sont ensuite comparées de façon automatisée avec d'autres banques de données afin par exemple de trouver des véhicules volés ou de poursuivre des criminels. La majeure partie des caméras RVS actuellement utilisées le sont par le Corps des gardes-frontière de la Confédération pour lutter contre la criminalité transfrontalière.
- *Exécution des peines :* la Suisse n'utilise pas (encore) d'applications d'intelligence artificielle pour la formation du jugement. Il faut cependant mentionner le programme ROS (exécution des sanctions axée sur le risque) utilisé dans toute la Suisse alémanique pour étudier la possibilité d'allégements dans l'exécution des peines. Pour ce faire, les données relatives à une personne tirées de l'extrait de casier judiciaire (par ex. âge, délits commis avant l'âge de 18 ans, nombre de condamnations antérieures ou ampleur des sanctions) sont transférées dans l'outil de screening des cas entièrement automatisé (FaST), qui procède à un classement dans trois catégories concernant le risque de fuite ou de récidive. Cette première appréciation sert de base pour décider si une analyse approfondie du risque individuel est requise ou non.

- **Cas 1 : décisions individuelles automatisées**

  L'art. 21, al. 1, nLPD définit la décision individuelle automatisée comme étant une « décision qui est prise exclusivement sur la base d'un traitement de données personnelles automatisé et qui a des effets juridiques pour elle ou l'affecte de manière significative ».

  Définition des termes :

  - **La décision repose exclusivement sur un traitement automatisé des données :** cela signifie que l'appréciation de la teneur des faits et la décision qui en découle sont

[37] Pour la recherche automatisée de véhicules et la surveillance du trafic (RVS) voir ATF **146** I 11.

issues d'une machine ou d'un algorithme, sans intervention d'une personne physique. Il est toutefois indifférent que la programmation de cet algorithme ait été assurée par une personne physique ou non. La décision individuelle automatisée peut reposer sur un algorithme simple appliquant une série de règles. Elle peut cependant être prise également par une application capable de développer et d'appliquer ses propres règles sur la base d'une grande quantité de données et des corrélations qu'elles contiennent (apprentissage automatique)[38]. Il y a également décision individuelle automatisée lorsque celle-ci est communiquée par une personne physique, qui ne l'a cependant pas prise elle-même[39].

Il convient de relever à ce propos qu'une interprétation de l'art. 21, al. 1, nLPD proche du libellé étendrait considérablement le champ d'application des dispositions relatives aux décisions individuelles automatisées. C'est pourquoi le Conseil fédéral a précisé dans son message du 15 septembre 2017 que seule une décision présentant **un certain degré de complexité** correspondait à la définition (► FF **2017** 6565, 6674). Le degré de complexité qu'une décision individuelle automatisée doit présenter n'est pas défini plus précisément dans le message. Toutefois, l'objectif de protection ressortant des dispositions ad hoc de la nLPD (notamment art. 21, art. 25, al. 2, let. f, et art. 34, al. 2, let. c, nLPD) permet de conclure qu'il est question spécialement des processus de décision qui ne sont pas intelligibles pour les personnes concernées[40]. Dans le sens d'une réduction téléologique de l'art. 21, al. 1, nLPD, il ne faudrait pas inclure dans la notion de décision individuelle automatisée les décisions triviales du type « si... donc » ou les interrogations « oui/non » concernant des critères objectifs et qui sont aisément compréhensibles pour la personne concernée. En font partie par exemple le retrait d'argent d'un avoir existant à un bancomat ou le contrôle de l'accès par carte à puce, sur la base d'une liste prédéfinie de personnes admises[41]. En outre, des opérations mathématiques simples (par ex. l'addition de valeurs) ne devraient pas être considérées comme étant d'un tel degré de complexité qu'elles constituent des décisions individuelles automatisées au sens de l'art. 21, al. 1, nLPD.

– **Effet de la décision :** pour qu'il y ait décision individuelle automatisée au sens de l'art. 21, al. 1, nLPD, elle doit avoir des effets juridiques pour la personne concernée ou l'affecter de manière significative.

  Une décision produit des effets juridiques si elle a des conséquences juridiques directes et prévues par la loi pour la personne concernée. Dans le domaine du droit privé, c'est le cas notamment pour la conclusion ou la dénonciation d'un contrat. En règle générale, il n'y a pas d'effets juridiques si un contrat n'est pas signé, car le statut juridique de la personne concernée reste inchangé (il y a toutefois une situation particulière dans le domaine des obligations contractuelles). Un contrat non conclu peut toutefois affecter l'intéressé de manière significative (deuxième cas de figure ; voir plus bas). Dans le domaine du droit public, il y a des effets juridiques notamment lorsqu'une décision est prise de manière entièrement automatisée (► FF **2017** 6565, 6674). Il n'est pas encore défini si des effets juridiques positifs répondent également à la définition de ce terme. La doctrine européenne et suisse le nie en partie en raison de l'objectif de protection de la norme, vu qu'il n'est pas nécessaire de protéger la personne concernée d'une

[38] Voir NADJA BRAUN BINDER/MATTHIAS SPIELKAMP/CATHERINE EGLI, in : Staatskanzlei Kanton Zürich (éd.), Einsatz Künstlicher Intelligenz in der Verwaltung, 28 février 2021, p. 19.

[39] Voir DAVID RECHSTEINER, Der Algorithmus verfügt. Verfassungs- und verwaltungsrechtliche Aspekte automatisierter Einzelentscheidungen, in : Jusletter du 26 novembre 2018, ch. 1 et 5 s.

[40] Concernant l'objectif de protection de l'art. 22 du règlement général de l'UE 2016/679 sur la protection des données, voir notamment MARTIN EBERS/CHRISTIAN A. HEINZE/TINA KRÜGEL/BJÖRN STEINRÖTTER (éd.), Künstliche Intelligenz und Robotik, Munich 2020, § 11, ch. 41 s.

[41] Concernant l'art. 22 du règlement général de l'UE 2016/679 sur la protection des données, voir SEBASTIAN SCHULZ, in : PETER GOLA (éd.), Kommentar zur DS-GVO, 2e éd., Munich 2018, Art. 22 DS-GVO ch. 20 ; GISELHER RÜPKE/KAI VON LEWINSKI/JENS ECKHARDT, Datenschutzrecht, Munich 2018, § 16, ch. 11 ; MARTIN EBERS/CHRISTIAN A. HEINZE/TINA KRÜGEL/BJÖRN STEINRÖTTER (éd.), op. cit., § 11, ch. 41 s.

décision qui lui est entièrement favorable. Vu que l'art. 21, al. 4, nLPD renvoie à l'art. 30, al. 2, de la loi fédérale sur la procédure administrative (PA), il serait également possible de conclure, en ce qui concerne les organes fédéraux, que dans le cas d'une décision individuelle automatisée correspondant entièrement aux souhaits de la personne concernée, seul le droit d'être entendu et d'exiger une révision par une personne physique selon l'art. 21, al. 2, nLPD serait supprimé, mais pas l'obligation d'informer selon l'art. 21, al. 1 et 4, nLPD.

Il y a lieu de supposer que la personne concernée est **affectée de manière significative** si elle subit des restrictions durables, par exemple de ses intérêts économiques ou personnels. De simples inconvénients ne sont pas suffisants. Tout dépend des circonstances concrètes du cas particulier. Il convient de tenir compte notamment de l'importance que le bien en question revêt pour la personne concernée, de la durabilité de l'effet de la décision, et il faut examiner si des alternatives sont possibles. Une personne concernée peut par exemple être affectée de manière significative si des prestations médicales sont attribuées sur la base de décisions automatisées (► FF **2017** 6565, 6674).

– **Rapport avec le profilage (► point 2.2.1, let. b))** : la décision individuelle automatisée doit être distinguée du profilage, même si ces deux procédés peuvent se recouper. Le traitement de données à la base d'une décision individuelle automatisée peut être un profilage, mais il ne l'est pas forcément[42]. Inversement, un profilage peut aboutir à une décision individuelle automatisée, mais pas impérativement (par ex. si le profilage sert uniquement à l'examen préalable, en vue d'une décision qui sera prise par une personne physique)[43].

– Les dispositions de la nLPD concernant les décisions individuelles automatisées mettent notamment en œuvre les exigences de l'art. 9, al. 1, let. a, de la Convention 108+ du Conseil de l'Europe ainsi que l'art. 11 de la directive UE 2016/680 relative à la protection des données dans le domaine pénal. En outre, la législation suisse sur la protection des données se rapproche ainsi du règlement général de l'UE 2016/679 sur la protection des données (art. 14, al. 2, let. g, et art. 22). Ces **réglementations européennes** doivent de ce fait être prises en compte lors de l'interprétation de la notion de décision individuelle automatisée.

À propos des exigences posées pour les bases légales :

– **Niveau normatif :** selon les circonstances, une décision individuelle automatisée peut entraîner une atteinte grave aux droits fondamentaux de la personne concernée au sens de l'art. 34, al. 2, let. c, nLPD, auquel cas une base légale doit être prévue dans une loi au sens formel (voir le message du Conseil fédéral du 15 septembre 2017 : ► FF **2017** 6565, 6696). C'est vrai tout spécialement lorsqu'une décision individuelle automatisée repose sur un profilage ou sur le traitement de données sensibles. En outre, il faut considérer dans quelle mesure et pour quelle durée la décision en question va se répercuter sur les droits de la personne concernée ou l'affecter d'une autre manière. Qui plus est, la règle suivante est applicable : plus une décision individuelle

[42] La teneur de l'art. 19, al. 1, P-LPD (après le vote final : art. 21, al. 1, nLPD) dans le projet du Conseil fédéral était la suivante : « Le responsable du traitement informe la personne concernée de toute décision qui est prise exclusivement sur la base d'un traitement de données personnelles automatisé, y compris le profilage, et qui a des effets juridiques sur la personne concernée ou qui l'affecte de manière significative. » L'insertion « y compris le profilage » a été supprimée par le Parlement. Cette suppression n'entraîne toutefois aucune modification matérielle (voir BO **2019** S 1241) ainsi que l'a expliqué la cheffe du DFJP au Conseil des États le 18 décembre 2019. Le profilage n'a pas de portée qui lui est propre dans cette disposition ; en effet, il entre dans le champ d'application respectivement de l'art. 19, al. 1, P-LPD ou de l'art. 21, al. 1, nLPD s'il aboutit à une décision individuelle automatisée, qu'il soit expressément mentionné ou non. Cette affirmation vaut pour le profilage « ordinaire » et pour le profilage à risque élevé selon l'art. 5, let. g, nLPD.

[43] Voir les « Lignes directrices relatives à la prise de décision individuelle automatisée et au profilage aux fins du règlement (UE) 2016/679 » du 6 février 2018 de l'ancien groupe de travail « Article 29 » sur la protection des données, pp. 8 s. avec des exemples.

automatisée est complexe, c'est-à-dire plus il est difficile pour la personne concernée d'en comprendre les tenants et les aboutissants, plus une base légale formelle sera impérative. Les décisions individuelles automatisées peuvent en outre être considérées comme des questions importantes, par ex. pour des raisons liées à l'organisation ou à la procédure, auquel cas l'art. 164, al. 1, let. g, Cst. exige une base légale au sens formel. Ainsi, une loi formelle est notamment nécessaire lorsqu'une procédure administrative se déroule exclusivement par voie électronique.

- **Densité normative :** la base légale doit prévoir expressément la décision individuelle automatisée ou la décrire de façon adéquate. Elle doit également préciser pour quels types de décisions l'automatisation complète est admise (par ex. décisions concernant une taxe) et quelles données sont traitées pour ce faire. Enfin, la personne concernée doit pouvoir comprendre, du moins dans les grandes lignes, selon quelle logique la décision est prise (par ex. type et pondération des données). C'est au cas par cas qu'il convient de déterminer si d'autres aspects doivent être mentionnés dans la base légale.

Autres effets juridiques des décisions individuelles automatisées :

En vertu de l'art. 21, al. 1 et 4, nLPD, il y a une **obligation d'informer** la personne concernée en cas de décision individuelle automatisée. Les organes fédéraux doivent qualifier en conséquence leurs décisions qui sont prises de cette manière. L'art. 21, al. 2, nLPD prévoit un droit pour la personne concernée de demander à **faire valoir son point de vue** et d'exiger que la décision soit **revue par une personne physique**. L'art. 21, al. 2, nLPD n'est pas applicable aux organes fédéraux lorsqu'ils ne sont pas tenus d'entendre la personne concernée avant la décision en vertu de l'art. 30, al. 2, PA ou d'une autre loi fédérale (par ex. si la décision individuelle automatisée peut être revue dans le cadre d'une procédure de recours non automatisée). Enfin, la personne concernée doit obtenir, dans le cadre de son **droit d'accès** selon l'art. 25, al. 2, let. f, nLPD, des informations sur l'existence d'une décision individuelle automatisée ainsi que sur la logique sur laquelle se base la décision. Si un organe fédéral est habilité à rendre des décisions individuelles automatisées, il faut **vérifier que toutes les exigences susmentionnées peuvent être remplies**.

Compatibilité avec le droit constitutionnel et procédural :

Lorsque l'administration fédérale recourt aux décisions individuelles automatisées, la question se pose de savoir si — indépendamment des exigences en matière de protection des données — ce mode de décision est compatible avec les principes de la Constitution et du droit administratif, et si oui dans quelles conditions. Il se peut en effet que d'autres restrictions à ce type de décisions découlent des garanties de procédure (art. 29 ss Cst. ; PA).

Quelques-unes des questions fondamentales soulevées par la doctrine, et qu'il convient d'approfondir, sont énumérées ci-après :

- **Maxime inquisitoire et obligation de collaborer** (art. 12 ss PA) : les exigences du droit de procédure posées pour la constatation des faits peuvent-elles être remplies dans le cas de décisions individuelles automatisées[44] ? Pour ces décisions, il est primordial que les données utilisées soient parfaitement correctes et présentent le degré de détail nécessaire. Cela vaut en particulier pour les données d'entraînement servant à l'apprentissage machine[45].

[44] NADJA BRAUN BINDER, Automatisierte Entscheidungen: Perspektive Datenschutzrecht und öffentliche Verwaltung, in : RSDA 2020, pp. 27 ss.

[45] NADJA BRAUN BINDER/CATHERINE EGLI/LAURENT FREIBURGHAUS/ELIANE KUNZ/NINA LAUKENMANN/LILIANE OBRECHT, in : Staatskanzlei Kanton Zürich (éd.), Einsatz Künstlicher Intelligenz in der Verwaltung, 28 février 2021, pp. 38 s.

- **Interdiction de la discrimination :** des défis importants se posent également eu égard à l'interdiction des discriminations. Dans les décisions individuelles automatisées — comme dans le cas de l'utilisation de l'intelligence artificielle en général —, le risque existe que des préjugés nés au fil du temps se cachent dans les jeux de données utilisés pour développer ou entraîner l'intelligence artificielle, ce qui peut renforcer des discriminations (inconscientes). D'où l'importance capitale de garantir la qualité des données. D'autres mesures pour éviter la discrimination pourraient consister à utiliser des algorithmes de contrôle analysant la pondération des facteurs à la base de la décision ou à prévoir des contrôles réguliers par d'autres institutions étatiques ou par des organisations tierces[46].
- **Droit à une décision motivée :** une autre question qui se pose en relation avec les décisions individuelles automatisées est celle de savoir comment garantir le droit à une décision motivée. Dans le cas d'un algorithme fondé sur des règles — fonctionnant de façon analogue à la pensée juridique chez les humains —, le système vérifie que certaines conditions sont remplies ; l'obligation de motiver ne devrait donc pas constituer un problème. Lorsque la décision individuelle automatisée repose sur l'intelligence artificielle, il est toutefois permis de douter qu'il soit possible de fournir une motivation juridique suffisante, car il est souvent difficile de comprendre le mode de fonctionnement des procédés d'apprentissage machine[47]. L'étude mandatée par le canton de Zurich sur l'utilisation de l'intelligence artificielle dans l'administration enjoint, pour les décisions prises à l'aide de l'intelligence artificielle, que soient précisés la logique appliquée par l'algorithme, le type et la quantité des données, l'intervalle de temps pendant lequel les données ont été réunies et comment elles sont pondérées ainsi que l'application de la logique de décision dans le cas concret. En outre, il peut être nécessaire de fournir des informations au sujet du groupe dans lequel l'algorithme classe la personne ainsi que sur les spécificités individuelles qui peuvent être déterminantes dans le cas particulier. Exceptionnellement, dans des circonstances particulières, la divulgation du code source de l'algorithme peut également être envisagée[48].
- **Pouvoir d'appréciation :** enfin, il est difficile de déterminer si des décisions individuelles automatisées sont possibles lorsque les autorités disposent d'un pouvoir d'appréciation. Une partie de la doctrine nie que ce soit possible. L'argumentation est qu'il est erroné sur le plan juridique qu'un organe fédéral renonce à exercer son pouvoir d'appréciation en émettant des décisions automatisées. Pour des motifs d'équité, il doit être possible de s'écarter des règles dans le cas particulier. Or, les algorithmes fondés sur des règles ne sont pas en mesure d'intégrer de telles marges de manœuvre. Si les algorithmes reposant sur l'apprentissage machine ne produisent pas de règles rigides, leur prise de décision repose exclusivement sur les décisions passées, ce qui va à l'encontre de l'appréciation correcte d'un cas individuel inconnu jusque-là[49].

- **Cas 2 : utilisation de l'intelligence artificielle à titre de soutien**

  Il n'y a pas décision individuelle automatisée au sens de l'art. 21, al. 1, nLPD lorsque seule la *préparation de la décision est automatisée*, mais qu'elle est ensuite prise par une personne physique. Il est probable que dans un proche avenir des systèmes reposant sur

[46] Voir NADJA BRAUN BINDER/CATHERINE EGLI/LAURENT FREIBURGHAUS/ELIANE KUNZ/NINA LAUKENMANN/LILIANE OBRECHT, in Staatskanzlei Kanton Zürich (éd.), Einsatz Künstlicher Intelligenz in der Verwaltung, 28 février 2021, pp. 39 ss.

[47] DAVID RECHSTEINER, op. cit., ch. 24 ss.

[48] NADJA BRAUN BINDER/CATHERINE EGLI/LAURENT FREIBURGHAUS/ELIANE KUNZ/NINA LAUKENMANN/LILIANE OBRECHT, in : Staatskanzlei Kanton Zürich (éd.), Einsatz Künstlicher Intelligenz in der Verwaltung, 28 février 2021, p. 38.

[49] DAVID RECHSTEINER, op. cit., ch. 28 ss. Voir aussi NADJA BRAUN BINDER/CATHERINE EGLI/LAURENT FREIBURGHAUS/ELIANE KUNZ/NINA LAUKENMANN/LILIANE OBRECHT, in : Staatskanzlei Kanton Zürich (éd.), Einsatz Künstlicher Intelligenz in der Verwaltung, 28 février 2021, pp. 46 ss, qui concluent également que l'intelligence artificielle ne doit pas être utilisée dans l'administration là où il existe un pouvoir discrétionnaire et une marge d'appréciation.

l'intelligence artificielle soient utilisés plus fréquemment pour fournir un soutien automatisé à la prise de décision. Les défis juridiques à relever en ce qui concerne les décisions individuelles automatisées se posent aussi de la même manière dans le cas de l'utilisation de l'intelligence artificielle à titre de simple soutien, même si les possibilités envisageables sont en partie différentes. Pour éviter les décisions discriminatoires, il est ainsi possible de veiller à ce que les personnes traitant les dossiers disposent des connaissances et des compétences nécessaires pour repérer les propositions discriminatoires de l'intelligence artificielle et prendre des décisions qui s'en écartent[50].

Lorsque l'intelligence artificielle utilisée à titre de soutien traite des données personnelles, il faut s'assurer qu'il existe une **base légale** répondant aux exigences de l'art. 34 nLPD à la fois en ce qui concerne le niveau et la densité de la norme. Si les modalités du traitement des données ou de l'utilisation de l'intelligence artificielle peuvent aboutir à des atteintes graves aux droits fondamentaux de la personne concernée, une base légale au sens formel doit être prévue selon l'art. 34, al. 2, let. c, nLPD. Pour ce qui est de la densité normative, ce sont les mêmes exigences qui s'appliquent que pour les décisions individuelles automatisées (► cas 1) et pour le profilage (► ch. 2.2.1, let. b)/dd) : la base légale doit indiquer notamment le but du recours à l'intelligence artificielle, les données qui sont utilisées par celle-ci et la logique sur laquelle repose l'application (par ex. type et pondération des données) ainsi que (le cas échéant) les caractéristiques de la personnalité qui sont évaluées. C'est au cas par cas qu'il convient de déterminer si d'autres aspects doivent être mentionnés dans la base légale.

2.2.2 Modes de communication des données : levée des exigences accrues relatives à la base légale pour la procédure d'appel

La procédure d'appel (« accès en ligne ») est une forme particulière de communication des données. Il s'agit d'une procédure automatisée permettant au destinataire des données de se procurer les données personnelles sans que l'organe fédéral propriétaire ne doive intervenir ou même sans qu'il remarque la consultation (« principe du libre-service »). En vertu de l'art. 19, al. 3, LPD en vigueur, les organes fédéraux ne sont en droit de rendre des données personnelles accessibles en ligne que si cela est prévu expressément dans la base légale. Les données sensibles (et les profils de la personnalité) ne peuvent être rendues accessibles en ligne que si une loi au sens formel le prévoit expressément.

Ces exigences accrues relatives aux bases légales pour les procédures d'appel sont abrogées par la révision totale de la LPD. On lit dans le message du Conseil fédéral du 15 septembre 2017 qu'elles apparaissent dépassées à l'ère de la société numérique (► FF **2017** 6565, 6698). En d'autres termes : l'exigence d'une base légale expresse a été abandonnée pour la procédure d'appel. Il va de soi que la communication des données en soi requiert toujours une base légale. Dans bien des cas d'ailleurs — surtout lorsqu'il y va d'atteintes graves aux droits fondamentaux — les impératifs de la transparence devraient imposer que la loi ou l'ordonnance mentionne qu'il s'agit d'un accès à des données, pour lequel le responsable du traitement reste passif (en l'occurrence, il est possible de parler d'« accès à des données/systèmes d'information », etc. au lieu de « procédures d'appel »). Il s'agit en outre de distinguer entre un « accès complet » et un simple « accès à l'index ». Par ailleurs, la règle demeure que la retenue est de mise lorsqu'il s'agit d'octroyer l'accès à des données, spécialement lorsque le but du système informatique concerné s'écarte considérablement du but poursuivi par le destinataire des données. En conséquence, il convient dans tous les cas d'envisager des modes de communication des données autres que l'accès par procédure d'appel.

[50] Voir NADJA BRAUN BINDER/CATHERINE EGLI/LAURENT FREIBURGHAUS/ELIANE KUNZ/NINA LAUKENMANN/LILIANE OBRECHT, in : Staatskanzlei Kanton Zürich (éd.), Einsatz Künstlicher Intelligenz in der Verwaltung, 28 février 2021, p. 42.

Outre la procédure d'appel, il existe trois autres modes de communication des données : la communication obligatoire (d'office ou sur demande), la communication spontanée et la communication sur demande et selon la libre appréciation de l'autorité sollicitée ; ► voir en particulier le Guide de législation (chapitre 14 ; ch. 834 ss). Ces formes de communication de données devront être mentionnées dans les bases légales, à l'avenir également, pour des raisons ne relevant pas uniquement de la protection des données.

3 Données des personnes morales

3.1 Contexte : Suppression de la protection des données concernant des personnes morales dans la nLPD

La révision totale de la LPD exclut du champ d'application de la loi à raison de la matière le traitement des données des personnes morales. L'art. 2, al. 1, nLPD prévoit que la loi ne régit plus que les données personnelles concernant des personnes physiques. En conséquence, les données personnelles sont définies comme étant « toutes les informations concernant une personne physique identifiée ou identifiable » (art. 5, let. a, nLPD). Les personnes morales restent protégées par d'autres dispositions de la législation suisse. Elles bénéficient de la protection de la personnalité en vertu du code civil (art. 28 ss du code civil), de la loi fédérale contre la concurrence déloyale, de la loi sur le droit d'auteur ou des dispositions concernant la protection du secret professionnel, d'affaires et de fabrication.

La levée de la protection des données des personnes morales dans la nLPD ainsi que la restriction de la notion de données personnelles à celles qui concernent des personnes physiques ont différentes répercussions sur le traitement des données par les organes fédéraux. Cette modification a notamment pour effet que les bases légales du droit fédéral habilitant les organes fédéraux à traiter et à communiquer des *données personnelles* ne seront plus applicables lorsque les *données* traitées ou communiquées se rapportent à des *personnes morales*. Cependant, en vertu du principe de légalité inscrit à l'art. 5, al. 1, Cst., toute action de l'État (y compris le traitement ou la communication de données) nécessite une base légale (voir aussi les art. 13, al. 2, 27 et 36, Cst.). En effet, la protection de la sphère privée vaut également pour les personnes morales (art. 13 Cst.), même si celles-ci ne sont pas titulaires de tous les aspects protégés par ce droit fondamental[51].

La révision totale de la LPD prévoit de ce fait une série de nouvelles dispositions dans la loi sur l'organisation du gouvernement et de l'administration (nLOGA ; ch. 13 de l'annexe 1/II de la nLPD), modifications qui régissent le traitement de données concernant des personnes morales par des organes fédéraux (art. 57*r* ss nLOGA ; ► point 3.2). En outre, la disposition transitoire de l'art. 71 nLPD doit combler les éventuelles lacunes juridiques pendant cinq ans (► point 3.3).

3.2 Nouvelles dispositions de la nLOGA relatives au traitement des données concernant des personnes morales

3.2.1 Définitions

Les principaux termes utilisés en rapport avec le traitement de données concernant des personnes morales par des organes fédéraux[52] sont définis ci-après. Pour ce faire, on s'est appuyé, par analogie, sur les dispositions de la LPD et de la nLPD. Les art. 57*r* ss nLOGA définissent uniquement la notion de « données sensibles concernant des personnes morales ».

- **Données (de personnes morales) :** par analogie à la notion de données personnelles (art. 5, let. a, nLPD), les données de personnes morales sont toutes les informations concernant une personne morale identifiée ou identifiable. Si la personne morale n'est pas au

[51] ATF **137** II 371, consid. 6.

[52] Le message du Conseil fédéral du 15 septembre 2017 (► FF **2017** 6565, 6733.) indique que la notion d'« organes fédéraux » dans les art. 57*r* ss nLOGA doit s'appuyer sur la définition légale donnée à l'art. 5, let. i, nLPD (« l'autorité fédérale, le service fédéral ou la personne chargée d'une tâche publique de la Confédération »).

moins identifiable (par ex. parce que les données ont été anonymisées), les dispositions des art. 57*r* ss nLOGA ne sont pas applicables.

- **Personnes morales :** il s'agit en premier lieu de toutes les associations de personnes organisées en corporations ainsi que des institutions indépendantes poursuivant un but particulier et jouissant de la personnalité juridique. En font partie les associations, les fondations, les sociétés par actions (ou sociétés anonymes), les sociétés en commandite par actions, les sociétés à responsabilité limitée, les coopératives ainsi que les corporations de droit privé régies par le droit cantonal et les institutions et corporations de droit public des cantons et de la Confédération. Dans la doctrine relative à la LPD actuelle, l'acception du terme « personne morale » est toutefois plus large. Par-delà le libellé de la loi, les sociétés de personnes sont également incluses ; même si elles n'ont pas de personnalité juridique propre, elles ont la capacité d'être partie et d'ester en justice (par ex. sociétés en nom collectif, sociétés en commandite et communautés de propriétaires par étage). Les nouveaux art. 57*r* ss nLOGA reposent également sur cette acception large de la notion de personne morale. Ne sont par contre pas incluses les associations de personnes qui ne présentent aucun des éléments de la personnalité juridique selon le droit suisse, par exemple les sociétés simples ou les communautés héréditaires[53].

- **Données sensibles concernant des personnes morales :** elles sont énumérées exhaustivement à l'art. 57*r*, al. 2, nLOGA. Il s'agit de :

  – données relatives à des poursuites ou des sanctions administratives ou pénales (let. a ; voir aussi art. 5, let. c, ch. 5, nLPD)

  – données relatives à des secrets professionnels, d'affaires ou de fabrication (let. b)[54].

  Le catalogue des données sensibles concernant des personnes morales est donc moins vaste que pour les personnes physiques, même s'il a été élargi pour inclure une nouvelle catégorie, « les données relatives à des secrets professionnels, d'affaires ou de fabrication ». Le besoin de protection des personnes morales est moins grand que celui des personnes physiques.

3.2.2 Traitement de données concernant des personnes morales (art. 57*r* nLOGA)

L'art. 57*r*, al. 1, nLOGA crée une base légale générale et directement applicable pour le *traitement* de données concernant des personnes morales. Il prévoit que les organes fédéraux ont le droit de traiter les données de personnes morales, y compris les données sensibles :

- dans la mesure où **l'accomplissement de leurs tâches l'exige** et

- dans la mesure où ces tâches sont **définies dans une loi au sens formel**. Une disposition dans une ordonnance ou une tâche qui pourrait être déduite de manière implicite ne suffisent pas. La tâche doit être clairement reconnaissable et déterminée de façon suffisamment précise.

Si les exigences de l'art. 57*r*, al. 1, nLOGA sont remplies, une habilitation dans une loi spéciale n'est pas nécessaire. Cette règle vaut pour le traitement aussi bien de données « ordinaires » concernant les personnes morales que de données sensibles à leur sujet. Ainsi, l'art. 57*r* nLOGA inclut d'une manière générale tous les types de traitement de données, y

[53] Sur l'ensemble de cette question, voir DAVID ROSENTHAL/YVONNE JÖHRI, Handkommentar DSG, N 6 ss. ad art. 2 LPD, BEAT RUDIN, SHK DSG, N 12 ad art. 2 LPD. Déjà dans le message du Conseil fédéral du 23 mars 1988 concernant la loi fédérale sur la protection des données, la notion de personne morale était entendue dans le sens exposé ci-dessus (FF **1988** II 421, 446).

[54] L'art. 57*r* nLOGA ne change rien aux actuelles dispositions pénales, administratives et de procédure relatives à la protection des secrets professionnels, d'affaires et de fabrication ; il n'est d'ailleurs applicable que dans la mesure où les organes fédéraux ont le droit de se procurer de telles données.

compris le profilage. La situation est toutefois différente si le but et le mode de traitement des données aboutissent à une atteinte telle aux droits fondamentaux de la personne morale concernée que l'art. 57*r* nLOGA ne parvient plus à satisfaire aux exigences du principe de la légalité en matière de densité normative selon les art. 5, al. 1, et art. 36, al. 1, Cst. Dans un tel cas de figure, une réglementation explicite est requise dans la loi spéciale.

Il convient de vérifier dans le cadre de chaque projet législatif si le traitement des données de personnes morales peut s'appuyer sur l'art. 57*r* nLOGA ou s'il faut créer une réglementation ad hoc. Il faut tout particulièrement veiller à décrire de façon suffisamment claire la tâche légale rendant nécessaire le traitement de données. En outre, il convient de vérifier si d'autres modalités du traitement doivent éventuellement être réglées (par exemple la durée de conservation ou les mesures techniques et organisationnelles visant à assurer la sécurité des données).

3.2.3 Communication de données concernant des personnes morales (art. 57*s* nLOGA)

L'art. 57*s*, al. 1, nLOGA prévoit que la *communication* de données concernant des personnes morales requiert une base légale dans une loi spéciale. À la différence de l'art. 57*r* nLOGA relatif au traitement des données concernant des personnes morales, l'art. 57*s* nLOGA ne constitue pas une base légale pour la communication de données spécifiques par les organes fédéraux. En l'occurrence, c'est le **principe de l'habilitation spéciale** qui s'applique.

L'art. 57*s* nLOGA règle la question de manière analogue à l'art. 36 nLPD (communication de données personnelles), en définissant en vertu de quelles bases légales un organe fédéral peut communiquer les données de personnes morales et les dérogations à ce principe :

- **Exigence d'une base légale :** d'une manière générale, les organes fédéraux n'ont le droit de communiquer les données de personnes morales que si une base légale le prévoit (art. 57*s*, al. 1, nLOGA). Cette base légale peut être contenue dans un traité international, dans une loi au sens formel ou dans une ordonnance. S'il suffit en règle générale de s'appuyer sur une **disposition dans une ordonnance** pour communiquer des données non sensibles concernant des personnes morales, la communication de données sensibles requiert une **base légale dans une loi au sens formel** (art. 57*s*, al. 2, nLOGA). Contrairement à l'art. 36, al. 1, en relation avec l'art. 34, al. 3, nLPD, l'art. 57*s* nLOGA ne prévoit pas expressément que la communication de données sensibles concernant des personnes morales peut s'appuyer sur une disposition contenue dans une ordonnance lorsque cette communication est indispensable à l'accomplissement d'une tâche légale formelle et que le motif du traitement ne présente pas de risque élevé pour les droits fondamentaux de la personne concernée. Cette lacune peut toutefois être comblée en appliquant cette réglementation par analogie. En effet, la nLOGA vise à régir le traitement des données de personnes morales de manière plus souple (et non plus stricte) que la nLPD.

- **Exceptions à l'exigence de la base légale :** l'art. 57*s*, al. 3, nLOGA énumère exhaustivement les cas où il est admissible de communiquer des données sensibles ou non concernant des personnes morales *sans disposer d'une base légale*. Ces exceptions sont les mêmes que celles qui sont inscrites à l'art. 36, al. 2, let. a et e, nLPD pour la communication de données personnelles (► point 2.1).

- **« Cas particuliers » :** l'art. 57*s*, al. 4 et 5, nLOGA prévoit, pour les personnes morales, la même réglementation particulière que l'art. 36, al. 3 et 5, nLPD en ce qui concerne la communication de données dans le cadre de l'information officielle du public (► point 2.1).

3.2.4 Droits des personnes morales (art. 57*t* nLOGA)

La suppression dans la nLPD de la protection des données concernant les personnes morales signifie que celles-ci ne peuvent plus faire valoir des prétentions en matière de protection des données. Ce changement concerne notamment le droit d'accès selon les art. 25 s. nLPD. C'est pourquoi l'art. 57*t* nLOGA renvoie aux règles de procédure applicables. Les personnes morales peuvent en conséquence consulter les pièces relatives à une procédure administrative de première instance (art. 26 ss PA), faire valoir leur droit d'être entendues (art. 29 ss PA) et faire au besoin recours contre la décision de l'organe fédéral compétent. Elles peuvent également invoquer l'art. 25*a* PA qui permet à toute personne qui a un intérêt digne de protection d'exiger de l'autorité compétente, pour des actes fondés sur le droit public fédéral et touchant à des droits ou des obligations, qu'elle émette une décision sujette à recours. Elles peuvent ainsi faire valoir leur droit à faire rectifier ou détruire leurs données par exemple.

Enfin, les personnes morales ont la possibilité de demander à consulter des documents officiels sur la base de la loi sur la transparence (LTrans). Cette loi applique le principe d'égalité en matière d'accès ; ce qui est révélé à une personne doit être accessible à toutes ("acces to one, access to all"). Toutefois, lorsqu'il s'agit de l'accès à leurs propres données, les personnes morales ne peuvent se voir opposer l'exception prévue à l'art. 7, al. 1, let. g, LTrans concernant les secrets professionnels, d'affaires ou de fabrication. Cette exception ne vaut que pour les tiers et non pour la personne morale requérante qui est maîtresse de ces secrets.

3.3 Dispositions transitoires relatives aux données de personnes morales (art. 71 nLPD)

La nouvelle réglementation de la protection des données concernant les personnes morales telle que décrite ci-dessus appelle la modification de nombreuses bases légales spéciales. Ces adaptations n'ont pas encore pu être réalisées dans le cadre de la révision de la LPD, ou de manière très ponctuelle seulement[55]. Il est prévu, après l'entrée en vigueur du nouveau droit sur la protection des données, de mettre en œuvre un projet coordonné par l'OFJ visant à réviser, de façon uniforme, toutes les dispositions du droit spécial afin de les adapter aux nouvelles exigences des art. 57*r* ss nLOGA.

Pour éviter les lacunes juridiques dans l'intervalle, une disposition transitoire concernant les organes fédéraux a été insérée à l'art. 71 nLPD. Elle précise que les dispositions d'autres actes de droit fédéral qui font référence à la protection des données[56] — qu'elles figurent dans des lois au sens formel ou matériel — continuent de s'appliquer au traitement des données concernant des personnes morales pendant les cinq ans suivant l'entrée en vigueur de la nLPD. Pendant ce délai, les organes fédéraux doivent pouvoir continuer de s'appuyer sur les bases légales en vigueur lorsqu'il s'agit de communiquer des données concernant des personnes morales. L'art. 71 nLPD vaut également pour les dispositions de protection des données du droit spécial qui entrent en vigueur après l'adoption ou l'entrée en vigueur de la nLPD.

L'application des dispositions transitoires de l'art. 71 nLPD n'est pas contraignante : si une unité administrative souhaite réglementer explicitement le traitement des données concernant

[55] Dans l'annexe 1/II de la nLPD, quelques lois fédérales ont déjà été vérifiées et adaptées pour des raisons liées à la sécurité du droit et à la praticabilité du traitement des données concernant des personnes morales. C'est le cas notamment de la LOGA, de la LTrans, de la loi fédérale sur la statistique fédérale ou de la loi sur la surveillance de la révision. Le message du Conseil fédéral du 15 septembre 2017 contient un aperçu détaillé de ces modifications, ► FF **2017** 6565, 6721 s. Les ordonnances correspondantes ont également été adaptées dans l'annexe 2 de l'OPDo. Une liste des ordonnances se trouve dans le rapport explicatif de l'ODPo du 31 août 2022 ► Rapport explicatif de l'OPDo, ch. 7.2.

[56] A contrario, le régime transitoire de l'art. 71 nLPD ne vaut pas pour les dispositions de la nLPD.

les personnes morales pendant la période transitoire de cinq ans, elle est bien sûr en droit de le faire.

4 Autres modifications découlant de la révision totale de la LPD

4.1 Acteurs du traitement des données : responsable du traitement et sous-traitant

La législation sur la protection des données prévoit différents acteurs, dont les rôles en matière de protection des données sont assortis de droits et d'obligations spécifiques. La réglementation de la nLPD, qui s'inspire du droit européen en matière de protection des données (voir art. 2, let. d et f, de la Convention 108+ du Conseil de l'Europe, l'art. 3, ch. 8 et 9, de la directive UE 2016/680 relative à la protection des données dans le domaine pénal ainsi que l'art. 4, ch. 8 et 9, du règlement général de l'UE 2016/679 sur la protection des données), utilise essentiellement les termes « responsable du traitement » et « sous-traitant ». Le « maître du fichier », terme utilisé jusqu'ici (art. 3, let. i, LPD), a été abandonné. Son rôle est toutefois transféré en large partie au « responsable du traitement ». Pour autant que l'on puisse en juger à l'heure actuelle, cette modification de la terminologie n'entraînera guère de changements matériels.

Les dispositions du droit spécial doivent définir clairement les différents acteurs participant au traitement de données et indiquer quel service en est responsable. En outre, il faudra que les personnes concernées puissent reconnaître les éventuels autres participants et leurs rôles respectifs. En l'occurrence, c'est uniquement la *relation en matière de protection des données* qui est déterminante, laquelle peut se distinguer de la « relation extérieure ». Dans le cas d'un mandat en vertu du droit des obligations par exemple, le mandant n'est pas forcément le responsable du traitement des données et le mandataire n'est pas forcément le sous-traitant.

- **Responsable du traitement** (art. 5, let. j, nLPD) : est considérée comme responsable du traitement, la personne qui, seule ou conjointement avec d'autres, détermine les finalités et les moyens du traitement des données. La décision concernant les moyens consiste essentiellement à définir les principaux paramètres du traitement ; il ne n'agit pas tant des moyens techniques et organisationnels, mais bien plus des facteurs qui sont déterminants pour l'admissibilité du traitement des données ou les risques qu'il peut présenter (par ex. quelles données sont traitées, de quelles sources proviennent-elles, pendant combien de temps et comment sont-elles traitées)[57]. Le responsable du traitement doit veiller au respect des exigences du droit sur la protection des données. Il est en outre chargé de protéger les droits des personnes concernées, en particulier leur droit d'accès (art. 25 s. nLPD).

- **Sous-traitant** (art. 5, let. k, nLPD) : si quelqu'un traite des données personnelles pour le compte du responsable du traitement, il est réputé sous-traitant, comme dans le droit en vigueur. La sous-traitance peut se dérouler notamment dans le cadre de l'utilisation de services en nuage (Cloud). Si des données sont dans le même temps rendues accessibles à l'étranger, les exigences des art. 16 ss nLPD doivent être remplies en sus. Le sous-traitant exécute pour l'essentiel le traitement des données selon les instructions du responsable du traitement. Les organes fédéraux peuvent également confier le traitement de données personnelles à des sous-traitants, sur la base d'un contrat ou de la loi (art. 9, al. 1, nLPD). La sous-traitance ne dégage pas le responsable du traitement de ses obligations en matière de protection des données. Celui-ci doit s'assurer activement — par le biais d'un choix judicieux du sous-traitant, des instructions données et du contrôle effectué —que les travaux sont effectués en conformité avec les exigences légales (en particulier en matière de sécurité des données), comme s'il s'en chargeait lui-même. L'externalisation du traitement des données ne doit pas altérer la position juridique de la personne concernée.

[57] DAVID ROSENTHAL, Controller oder Processor : Die datenschutzrechtliche Gretchenfrage, in : Jusletter du 17 juin 2019, ch. 33.

Si les conditions d'une sous-traitance sont remplies, le sous-traitant est assimilé au responsable du traitement en ce qui concerne la protection des données. Dans ce cas, le sous-traitant n'est plus un tiers (voir plus bas). Aucune modification sensible n'a été apportée aux conditions de la sous-traitance dans le cadre de la révision totale de la loi (voir art. 9 nLPD). Ce qui est nouveau, c'est que le sous-traitant ne peut lui-même sous-traiter un traitement à un tiers qu'avec l'autorisation préalable du responsable du traitement (art. 9, al. 3, nLPD). Cette autorisation préalable peut être de nature spécifique ou générale (voir art. 7, al. 1 et 2, OPDo).

- **Traitement de données conjoint** (art. 33 nLPD) : si plusieurs organes fédéraux traitent des données personnelles conjointement ou en collaboration avec des organes cantonaux ou des personnes privées, des questions délicates de délimitation des responsabilités peuvent se poser[58]. Pour éviter ces difficultés, l'art. 33 nLPD prévoit que le Conseil fédéral règle dans ce cas les procédures de contrôle et les responsabilités. Cette disposition correspond en grande partie à l'actuel art. 16, al. 2, LPD. À la différence du droit en vigueur, le Conseil fédéral n'est plus seulement habilité à formuler des règles concernant le contrôle et la responsabilité en matière de protection des données, mais il en a l'obligation. L'OPDo ne contient pas de prescription à ce sujet. Il revient aux organes fédéraux de le faire dans leur législation spéciale. Il s'agit également de clarifier des questions telles que les droits d'accès aux données, la sécurité des données et la mise en œuvre des droits des personnes concernées par le traitement des données.

- **Tiers :** la notion de tiers n'est pas définie explicitement dans la nLPD. En s'appuyant sur le règlement général de l'UE 2016/679 sur la protection des données (art. 4, ch. 10), on peut dire que le tiers est une personne privée, un organe fédéral ou cantonal, qui n'est ni responsable du traitement ni sous-traitant. Le sous-traitant n'est par conséquent plus considéré comme un tiers dans la nLPD, à la différence de l'art. 10*a* LPD. En effet, il cesse d'être un tiers à compter du moment où il débute ses activités contractuelles pour le compte du responsable du traitement (► FF **2017** 6565, 6643).

    - **Destinataire :** un destinataire est une personne privée, un organe fédéral ou cantonal auquel des données personnelles sont communiquées, peu importe qu'il s'agisse d'un tiers ou non (voir art. 2, let. d, de la Convention 108+ du Conseil de l'Europe, l'art. 3, ch. 10, de la directive UE 2016/680 relative à la protection des données dans le domaine pénal et l'art. 4, ch. 9, du règlement général de l'UE 2016/679 sur la protection des données [les deux derniers prévoyant des exceptions pour les autorités qui obtiennent certaines données personnelles dans le cadre d'une mission d'enquête particulière]). Les sous-traitants (ou les coresponsables) sont donc également considérés comme des destinataires.

[58] Pour ces questions de délimitation, voir le droit européen de protection des données « Guidelines 07/2020 on the concepts of controller and processor in the GDPR » du Comité européen de la protection des données (EDPB).

4.2 Communication de données à l'étranger

Comme c'est déjà le cas dans le droit en vigueur (art. 6 LPD), la nLPD prévoit des exigences spéciales pour la communication de données personnelles à l'étranger (art. 16 s. nLPD). La révision totale de la LPD subit toutefois les modifications suivantes :

- **Niveau adéquat de protection des données :** l'art. 16, al. 1, nLPD dispose que les données personnelles ne peuvent être communiquées à l'étranger que si la législation de l'État concerné ou que l'organisme international garantit un niveau de protection adéquat. Il appartient *nouvellement* au Conseil fédéral de constater de manière contraignante quels pays ou quels organismes internationaux assurent un tel niveau de protection. Les critères selon lesquels le Conseil fédéral doit évaluer les législations étrangères sont précisés dans l'ordonnance (art. 8 OPDo). Les États assurant un niveau adéquat de protection des données sont énumérés dans l'annexe 1 OPDo.

- **Garanties appropriées pour assurer la protection des données :** l'art. 16, al. 2, nLPD dispose que des données personnelles peuvent être communiquées à un État ne figurant pas sur la liste du Conseil fédéral lorsqu'un niveau de protection approprié[59] est garanti par d'autres instruments. Ces derniers incluent les traités internationaux (let. a), les clauses contractuelles de protection des données (let. b), les garanties spécifiques élaborées par des organes fédéraux (let. c), les clauses types de protection des données (let. d) et les règles d'entreprise contraignantes en matière de protection des données (« binding corporate rules » ; let. e). Les contenus minimaux de ces garanties sont définis dans l'ordonnance (art. 9 à 11 OPDo). L'OPDo prévoit encore deux autres types de garanties : les codes de conduite et les certifications (art. 12 OPDo et art. 16, al. 3 nLPD). Il y a obligation de communiquer préalablement certaines de ces garanties au PFPDT (art. 16, al. 2, let. b et c, nLPD) ou de les lui faire approuver (art. 16, al. 2, let. d et e, nLPD ainsi qu'art. 12, al. 2, OPDo). Les garanties adéquates prévues à l'art. 16, al. 2, nLPD correspondent en grande partie à celles du droit en vigueur (art. 6, al. 2, let. a et g, et al. 3, LPD). Il y a toutefois quelques modifications du contenu. Pour les nouveautés, nous renvoyons au message du Conseil fédéral du 15 septembre 2017 (► FF **2017** 6565, 6658 ss).

  Dans ce contexte, il convient par conséquent de prêter une attention toute particulière, lors de la **conclusion de traités internationaux**, à ce qu'un niveau de protection suffisant soit garanti à l'étranger. Les éléments centraux sont le respect des principes de la protection des données, les droits des personnes concernées (tels que le droit d'accès, d'opposition, d'effacement et de rectification, avec les voies de droit correspondantes), les exigences eu égard à une éventuelle communication ultérieure à l'étranger ainsi que la surveillance indépendante de la protection des données.

  - **Dérogations** (art. 17 nLPD) : comme c'est le cas dans le droit en vigueur (art. 6, al. 2, let. b à f, LPD), la nLPD prévoit à l'art. 17 différentes dérogations permettant de communiquer des données à l'étranger même en l'absence d'une protection adéquate des données selon l'art. 16, al. 1, nLPD et de garanties de protection appropriées selon l'art. 16, al. 2 et 3, nLPD. Les dérogations prévues à l'art. 17, al. 1, let. a à e nLPD ont été reprises du droit en vigueur et ne subissent que des adaptations mineures, qui sont expliquées dans le message du Conseil fédéral du 15 septembre 2017 (► FF **2017** 6565, 6661 s.). L'art. 17, al. 1, let. f, nLPD est nouveau en revanche. Cette disposition permet la communication de données personnelles en l'absence d'une protection adéquate des données, lorsque les données proviennent d'un registre prévu par la loi,

[59] Dans son arrêt du 16 juillet 2020 dans l'affaire C-311/18 (« Schrems II »), la Cour de justice de l'Union européenne a retenu que les garanties appropriées doivent être de nature à assurer un niveau de protection substantiellement équivalent à celui garanti au sein de l'Union européenne (donc : adéquat) (ch. 96).

accessible au public, pour autant que les conditions qui y sont énumérées soient remplies.

4.3 Analyse d'impact relative à la protection des données

L'**analyse d'impact relative à la protection des données** doit permettre aux responsables du traitement (organes fédéraux et personnes privées) d'identifier les risques à un stade précoce et de prendre au besoin des mesures de protection appropriées. Une telle analyse doit être établie lorsque le traitement de données envisagé est susceptible d'entraîner un risque élevé pour la personnalité ou les droits fondamentaux de la personne concernée (art. 22, al. 1, nLPD). La nLPD donne comme exemple d'un risque élevé un traitement à grande échelle de données sensibles (art. 22, al. 2, nLPD). L'analyse d'impact doit indiquer quel traitement des données est prévu, ses risques pour la personnalité ou pour les droits fondamentaux ainsi que les mesures de protection qui ont déjà été prises ou qui doivent l'être (art. 22, al. 3, nLPD). Si, en dépit des mesures mises en œuvre ou prévues, il reste encore un risque résiduel élevé pour la personnalité ou les droits fondamentaux de la personne concernée, il faut **consulter le PFPDT** (art. 23, al. 1, nLPD). Celui-ci communique ses éventuelles objections concernant le traitement de données prévu et peut proposer lui-même des mesures de protection appropriées. Pour les organes fédéraux, l'analyse d'impact ne devrait pas constituer qu'une nouveauté partielle. En vertu de l'art. 20, al. 2, OLPD, ils doivent en effet annoncer aujourd'hui déjà au conseiller à la protection des données ou au PFPDT tous les projets de traitement automatisé de données afin que les exigences de la protection des données soient prises en considération. Pour les organes fédéraux, les exigences relatives à l'établissement d'une analyse d'impact relative à la protection des données doivent être coordonnées avec les processus déjà en place, notamment la méthode de gestion de projets HERMES.

Il est prévu à l'avenir de coordonner cette analyse avec la **procédure législative**. Si le traitement de données par un organe fédéral requiert des modifications d'une base légale et si les conditions pour une analyse d'impact relative à la protection des données sont remplies, celle-ci doit être remise au Conseil fédéral avec la proposition du projet législatif (au besoin avec une prise de position du PFPDT). Les résultats de l'analyse (et l'éventuelle prise de position du PFPDT) doivent en outre être publiés dans le message du Conseil fédéral.

4.4 Adaptations terminologiques

4.4.1 Préposé fédéral à la protection des données et à la transparence

De nouvelles abréviations sont introduites par la révision totale de la LPD pour désigner le « Préposé fédéral à la protection des données et à la transparence ». Elles devront également être utilisées dans les dispositions sur la protection des données des lois spéciales :

- Le Préposé fédéral à la protection des données et à la transparence en tant qu'**autorité** est abrégé « PFPDT » (voir art. 4, al. 1, nLPD)
- Lorsqu'il est question de la **personne physique** en revanche, à savoir la cheffe ou le chef du PFPDT, le terme de « préposé » est utilisé (voir art. 43, al. 1, nLPD).

Exemple : modification de la loi sur le Parlement au ch. 12 de l'annexe 1/II de la nLPD (nLParl)

Art. 40*a*, al. 1, let. d, nLParl : « La Commission judiciaire est compétente pour préparer l'élection et la révocation des personnes suivantes : *le chef du Préposé fédéral à la protection des données et à la transparence (préposé)*».

Art. 142, al. 2, nLParl : « Il [le Conseil fédéral] reprend tels quels dans son projet de budget et dans le compte d'État les projets de budget et les comptes de l'Assemblée fédérale, des tribunaux fédéraux, du Contrôle fédéral des finances, du Ministère public de la Confédération, de l'Autorité de surveillance du Ministère public de la Confédération et *du Préposé fédéral à la protection des données et à la transparence (PFPDT)* ».

4.4.2 Maître du fichier/Fichier

- Le terme « **maître du fichier** » est remplacé par « **responsable du traitement** » (voir point 4.1).

- En outre, la nLPD renonce à l'utilisation du terme « **fichier** ». L'actuelle LPD, qui rattache différents droits et obligations à l'existence d'un fichier (par ex. droit d'accès selon l'art. 8 LPD), définit ce terme comme suit dans son art. 3, let. g : « tout ensemble de données personnelles dont la structure permet de rechercher les données par personne concernée ». Cette description remonte à une époque où les fichiers se trouvaient encore en majeure partie sous la forme de fiches carton ou dans des classeurs. Au vu des possibilités technologiques actuelles (de recherche), il faut partir du principe que pratiquement tout répertoire électronique constitue un fichier au sens de la LPD. Ce terme est de ce fait dépassé. La responsabilité en matière de protection des données sera dès lors rattachée au fait de traiter des données personnelles. Dans l'annexe 1/II de la nLPD, le terme « fichier » a été systématiquement abandonné dans les dispositions sur la protection des données des législations spéciales, et remplacé par des termes adaptés au contexte.

  Exemples : traiter des données personnelles, (activités de) traitement de(s) données, banque de données, infrastructure électronique, système informatisé, collecte de données.

  Il convient de veiller à ne plus utiliser le terme « fichier » dans des dispositions sur la protection des données, qu'elles soient nouvelles ou révisées.

4.4.3 Données sur les poursuites ou les sanctions pénales et administratives

La modernisation de la terminologie à l'art. 5, let. c, ch. 5, nLPD (définition des données sensibles) ne concerne que la version allemande. L'expression « Daten über administrative oder strafrechtliche Verfolgungen und Sanktionen » (art. 3, let. c, ch. 4, LPD) a été remplacée par « Daten über *verwaltungs*- und strafrechtliche Verfolgungen oder Sanktionen ». Cette adaptation doit également être prise en compte dans les dispositions sur la protection des données dans les lois spéciales.

Exemples : Art. 65, al. 2, art. 101, al. 1, et art. 110 de la loi révisée sur les jeux d'argent (ch. 90 de l'annexe 1/II de la nLPD).

4.5 Survol des autres contenus de la révision totale de la LPD

En plus des modifications présentées dans la première partie du présent document, et qui sont particulièrement importantes pour les projets législatifs de l'administration fédérale, la révision totale de la LPD a entraîné de nombreux autres changements dans la protection des données (résumé sommaire, aperçu non exhaustif).

- **Champ d'application de la nLPD :**
  - *Champ d'application à raison de la matière :*
    - La révision totale de la LPD exclut du champ d'application de la loi à raison de la matière le **traitement de données concernant des personnes morales**, ► point 3.
    - Plus aucune exception au champ d'application de la LPD n'est prévue pour les procédures civiles (en cours), les procédures pénales, les procédures d'entraide judiciaire internationale ou les procédures de droit public ou administratif. En lieu et place, l'art. 2, al. 3, nLPD régit la **relation entre droit de procédure et loi sur la protection des données :** les traitements de données personnelles effectués dans le cadre de procédures devant des tribunaux ou dans le cadre de procédures régies par des dispositions fédérales de procédure, ainsi que les droits des personnes concernées, obéissent au droit de procédure applicable. Les dispositions de la nLPD s'appliquent aux procédures administratives de première instance (comme c'est le cas de la LPD actuellement). Voir à ce propos les explications dans le message du Conseil fédéral du 15 septembre 2017, ► FF **2017** 6565, 6633 ss. Pour les exceptions à la surveillance par le PFPDT, voir art. 4, al. 2, let. c à e, nLPD.
    - La nLPD ne prévoit plus non plus d'exclusion du champ d'application pour les **registres publics relatifs aux rapports de droit privé**. L'art. 2, al. 4, nLPD prévoit toutefois que ces registres (notamment l'accès à ces registres et les droits des personnes concernées) sont régis par les dispositions spéciales du droit fédéral applicable. Si ces dispositions ne contiennent aucune réglementation à ce sujet, la nLPD s'applique par défaut. Voir à ce propos les explications dans le message du Conseil fédéral du 15 septembre 2017, ► FF **2017** 6565, 6635 ss. Les registres publics relatifs aux rapports de droit privé qui sont tenus par des autorités fédérales sont désormais soumis à la surveillance du PFPDT (art. 4, al. 1, nLPD).
  - *Champ d'application territorial :* le Parlement a inséré une réglementation explicite sur le **champ d'application territorial** à l'art. 3 nLPD, disposition qui ne devrait toutefois pas entraîner de modifications matérielles. Pour les *dispositions de protection des données relevant du droit privé et du droit pénal*, l'art. 3, al. 2, nLPD renvoie de manière déclaratoire aux normes de conflit existantes dans la loi fédérale sur le droit international privé (art. 139 LDIP) et dans le code pénal (art. 3 ss CP). Pour les *dispositions de protection des données relevant du droit public* (y compris la surveillance par le PFPDT), l'art. 3, al. 1, nLPD fixe que la loi sur la protection des données est applicable aux états de fait qui déploient des effets en Suisse, même s'ils se sont produits à l'étranger. Cette réglementation n'a rien de nouveau en soi non plus. Elle codifie simplement la pratique des tribunaux concernant les principes de territorialité et les principes des effets en droit public[60].
  - *Champ d'application personnel :* aucune modification.

    La nLPD reste applicable au traitement de données personnelles par des *personnes privées* et par des *organes fédéraux* (art. 2, al. 1, let. a et b, nLPD). Les organes fédéraux sont des autorités ou des services

[60] Voir concernant le droit sur la protection des données, ATF **138** II 346 dans l'affaire « Google Street View ».

de la Confédération ou des personnes chargées d'une tâche publique de la Confédération (art. 5, let. i, nLPD). Le traitement de données par des *autorités cantonales ou communales* est soumis à la législation cantonale, peu importe que l'autorité collecte les données directement ou qu'elle se les procure par un accès en ligne à des banques de données de la Confédération. Le traitement de données par des organes cantonaux dans le cadre de l'exécution du droit fédéral est d'une manière générale soumis également au droit cantonal[61]. Pour quelques domaines relevant de la compétence de la Confédération, il existe une réglementation spéciale en matière de protection des données, par exemple dans le domaine des assurances sociales ; cette réglementation s'applique aussi bien aux autorités fédérales compétentes qu'aux autorités cantonales chargées de l'exécution du droit fédéral. Dans ce cas, la Confédération doit toutefois tenir compte du droit d'organisation cantonal[62].

- **Remplacement du registre des fichiers par le registre des activités de traitement :** à l'avenir, les responsables du traitement du secteur privé et les organes fédéraux devront tenir un registre de leurs activités de traitement. Les organes fédéraux doivent déclarer ces registres au PFPDT (art. 12, al. 1 et 4, nLPD). Le PFPDT tient un registre officiel de ces activités, qui est publié (art. 56 nLPD).

  Le registre des activités de traitement remplace l'actuelle déclaration des fichiers au PFPDT (art. 11*a* LPD). Le contenu minimum du registre est défini à l'art. 12, al. 2 (responsable du traitement) et al. 3 (sous-traitant), nLPD. Les informations devant être fournies dans le registre des activités de traitement du responsable du traitement sont un peu plus étendues que celles qui sont exigées aujourd'hui pour la déclaration des fichiers. Ainsi, il faut indiquer non seulement la finalité du traitement, les catégories des données personnelles traitées et les destinataires des données, mais également (si possible) des renseignements sur le délai de conservation, les mesures visant à garantir la sécurité des données et les éventuelles garanties de protection en cas de communication de données à l'étranger.

  Si des dérogations à l'obligation de tenir un registre sont prévues pour les responsables du traitement du secteur privé (art. 12, al. 5, nLPD et art. 24 OPDo), la nLPD n'admet aucune exception pour les organes fédéraux. Si un organe fédéral doit être exempté de l'obligation d'établir un tel registre ou de déclarer le registre au PFPDT, cette exception doit être réglementée dans la loi spéciale applicable.

  Exemples : art. 11, al. 2, de la loi sur la géoinformation (ch. 41 de l'annexe 1/II de la nLPD) ou art. 99, al. 3, let. d, et art. 100, al. 4, let. c, ch. 2, de la loi sur l'armée (ch. 40 de l'annexe 1/II de la nLPD).

- **Extension des obligations des responsables du traitement :**

  – *Devoir d'informer lors de la collecte de données personnelles :* la révision totale de la LPD étend le devoir d'informer à la collecte de *tous les types de données personnelles* (art. 19, al. 1, nLPD). Cette exigence n'a rien de nouveau pour les organes fédéraux (art. 18*a* LPD). La modification concerne donc essentiellement des responsables du traitement privés, qui n'ont aujourd'hui un devoir d'informer que lors de la collecte de données sensibles ou de l'établissement de profils de la personnalité. Le devoir d'informer continue de s'appliquer également lorsque les données ne sont pas collectées auprès de la personne concernée, mais auprès de tiers. L'art. 19, al. 2, phrase introductive, nLPD dispose qu'il faut d'une manière générale communiquer à la personne concernée toutes les informations nécessaires pour qu'elle puisse faire valoir ses droits

[61] La disposition actuellement en vigueur, l'art. 37, al. 1, LPD, prévoit que le traitement de données personnelles par des organes cantonaux en exécution du droit fédéral est régi par les dispositions des art. 1 à 11*a*, 16, 17, 18 à 22 et 25, al. 1 à 3, LPD s'il n'existe pas de dispositions cantonales de protection des données assurant un niveau de protection adéquat ; cette disposition est abrogée par la révision totale de la LPD.

[62] Voir le rapport du 22 décembre 2010 du Conseil fédéral en exécution du postulat Lustenberger 07.3682 « Échange de données personnelles entre autorités fédérales et autorités cantonales » (FF **2011** 615, 623 s.).

prévus dans la nLPD et pour garantir la transparence du traitement. L'art. 19, al. 2, let. a à c, et al. 3 et 4, nLPD concrétise ce principe, en précisant quelles sont les indications minimales à fournir. Cette conception de la réglementation permet de gérer le devoir d'informer de manière souple et suit une approche fondée sur les risques. Les *exceptions au devoir d'informer et les restrictions* sont définies à l'art. 20 nLPD. Pour les organes fédéraux, c'est principalement l'art. 20, al. 1, let. b, nLPD qui est important. Selon cette disposition, l'obligation d'informer ne s'applique pas à un traitement de données qui est prévu par la loi. Il est dès lors essentiel que la personne concernée puisse reconnaître les éléments clés du traitement de données dans la base légale (► point 2).

- *Analyse d'impact relative à la protection des données :* ► point 4.3.

- *Obligation d'annoncer les violations de la sécurité des données :* l'art. 24, al. 1, nLPD contient une nouveauté, à savoir une obligation d'annoncer dans les meilleurs délais au PFPDT les violations de la sécurité des données entraînant vraisemblablement un risque élevé pour la personnalité ou les droits fondamentaux de la personne concernée. Dans certaines circonstances, les personnes concernées doivent être directement informées elles aussi (art. 24, al. 4, nLPD). La violation de la sécurité des données est définie à l'art. 5, let. h, nLPD : « 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 ».

- *Obligations spéciales en cas de décision individuelle automatisée :* ► point 2.2.1, let. c).

- **Droits des personnes concernées :**

  - *Droit d'accès :* la réglementation aux art. 25 ss nLPD correspond en majeure partie à celle des art. 8 ss LPD. Cependant, le *catalogue des informations à fournir* est élargi (art. 25, al. 2, nLPD). Il faudra à l'avenir renseigner également sur la durée de conservation des données personnelles ou, si cette condition ne peut pas être satisfaite, indiquer les critères pour fixer cette durée (let. b) ; en outre, il faudra préciser s'il y a décision individuelle automatisée (► point 2.2.1, let. c)/cc) et si oui, sur quelle logique elle se fonde (let. f). La *restriction au droit d'accès* prévue à l'art. 26, al. 1, let. c, nLPD est également nouvelle. En vertu de cette disposition, le droit d'accès peut être refusé, restreint ou la communication des renseignements peut être différée, si la demande est manifestement infondée, notamment si elle poursuit un but *contraire à la protection des données* ou si elle est manifestement procédurière. Selon la jurisprudence du Tribunal fédéral, il y a un but contraire à la protection des données par exemple lorsque les données servent à se renseigner sur une éventuelle partie adverse ou à faire l'économie des frais liés à l'obtention des preuves[63].

  - *Portabilité des données :* le Parlement a introduit aux art. 28 s. nLPD un droit à la remise et à la transmission de données (= portabilité des données). L'art. 28, al. 1, nLPD fixe que la personne concernée peut demander au responsable du traitement qu'il lui remette, dans un format électronique couramment utilisé, les données personnelles la concernant qu'elle lui a communiquées. La personne concernée peut en outre demander au responsable du traitement qu'il transmette les données personnelles la concernant à un autre responsable du traitement, pour autant que cela n'exige pas des efforts disproportionnés. Il faut partir du principe que ce droit à la portabilité des données sera applicable avant tout dans le secteur du droit privé, vu que ces deux prétentions

[63] Voir ATF **138** III 425, consid. 5.4 s.

n'existent que lorsqu'il s'agit de données traitées avec le consentement de la personne concernée ou qui sont en relation directe avec la conclusion ou l'exécution d'un contrat entre elle et le responsable du traitement. Les restrictions du droit à la remise ou à la transmission des données sont définies à l'art. 29 nLPD.

- D'*autres droits* sont réglés à l'art. 37 nLPD (opposition à la communication de données personnelles) et à l'art. 41 nLPD (par ex. droit à l'effacement ou à la destruction de données personnelles traitées illicitement). Ces droits correspondent pour l'essentiel à ceux du droit en vigueur (art. 20 et 25 LPD). Ce qui est nouveau, c'est le droit à limiter le traitement des données (art. 41, al. 3, nLPD). Pour les autres modifications, voir le message du Conseil fédéral du 15 septembre 2017, ► FF **2017** 6565, 6699 ss.

- **Préposé fédéral à la protection des données et à la transparence (PFPDT) :**
  - **Élection du chef du PFPDT :** le chef du PFPDT (► point 4.4.1) est nommé par le Conseil fédéral selon le droit en vigueur, nomination qui est ensuite approuvée par l'Assemblée fédérale (art. 26, al. 1, LPD) ; à l'avenir, c'est l'Assemblée fédérale qui élira seule le préposé (art. 43, al. 1, nLPD). Cette modification appelle différentes adaptations de la réglementation sur l'organisation et le personnel, par exemple en ce qui concerne le budget du PFPDT (art. 45 nLPD). En outre, l'Assemblée fédérale a adopté une ordonnance sur les rapports de travail du chef du PFPDT (► FF **2022** 348 ; voir également l'initiative parlementaire 21.443 de la CIP-N). Le PFPDT continue cependant à constituer une unité administrative décentralisée (sans personnalité juridique), qui est rattachée administrativement à la Chancellerie fédérale (art 43, al. 4, nLPD ; art 2, al. 3, LOGA ; art. 7*a*, al. 1, let. b, et annexe 1, let. A, ch. 2.1.1 de l'ordonnance sur l'organisation du gouvernement et de l'administration).
  - **Enquêtes concernant les violations des prescriptions de protection des données :** dans le sillage de la révision totale de la LPD, les compétences du PFPDT en matière de surveillance sont renforcées. À l'avenir, le PFPDT devra ouvrir une enquête, d'office ou sur dénonciation, lorsqu'un nombre suffisant d'indices font penser qu'un traitement de données pourrait être contraire à des dispositions de protection des données (art. 49, al. 1, nLPD). Cette réglementation lui octroie de plus vastes compétences qu'aujourd'hui pour intervenir notamment auprès de responsables du traitement du secteur privé (voir art 29, al. 1, LPD, en vertu duquel il devait y avoir notamment une erreur de système pour que le PFPDT puisse enquêter dans le secteur privé). Le PFPDT peut toutefois renoncer à ouvrir une enquête lorsque la violation des prescriptions de protection des données est de peu d'importance (art. 49, al. 2, nLPD). L'art. 50 nLPD élargit l'éventail d'instruments à la disposition du PFPDT pour constater les faits, si le responsable du traitement (organe fédéral ou personne privée) ne respecte pas son obligation de collaborer. S'il y a violation des prescriptions de protection des données, le PFPDT pourra à l'avenir **ordonner** des mesures administratives (et pas seulement les recommander), en vertu de l'art. 51 nLPD. Cette compétence vaut aussi bien pour les responsables du traitement privés que pour les organes fédéraux. La procédure d'enquête et les décisions du PFPDT sont régies par la PA (art. 52, al. 1, nLPD).
  - **Législation :** le PFPDT va continuer à jouer un rôle important dans les travaux législatifs. En vertu de l'art. 58, al. 1, let. e, nLPD, il se prononce sur les projets d'actes législatifs et les mesures de la Confédération qui impliquent un traitement de données.
- **Extension des dispositions pénales :** les éléments constitutifs de l'infraction en matière de protection des données sont élargis dans les art. 60 ss nLPD ; la limite supérieure des amendes est portée de 10 000 francs à 250 000 francs. Il convient en particulier d'attirer

l'attention sur le nouvel art. 63 nLPD, qui prévoit des sanctions lorsqu'une personne, intentionnellement, ne se conforme pas à une décision du PFPDT ; cette disposition confère donc au PFPDT une sorte de possibilité de sanction « indirecte ». Le PFPDT peut en outre dénoncer des infractions aux autorités de poursuite pénale compétentes et faire valoir les droits d'une partie plaignante dans la procédure pénale (art. 65, al. 2, nLPD). Cette mesure n'affecte toutefois pas les organes fédéraux, car les dispositions pénales de la nLPD s'appliquent uniquement aux responsables du traitement privés (comme c'est le cas actuellement, en vertu de la LPD).