GUIDE DE LEGISLATION
en matière de PROTECTION DES DONNEES

Conséquences de la nouvelle loi sur la protection des données sur l'élaboration de bases légales

Berne, août 2022, actualisation en mars 2024

Table des matières

Introduction

A) Contexte

Le présent document remplace le Guide pour l'élaboration des bases légales nécessaires pour permettre à un organe fédéral d'exploiter un système de traitement automatisé de données personnelles du 16 décembre 2010 devenu obsolète. L'objectif est de présenter, sous une forme résumée, les conséquences qu'entraîne la révision totale de la loi fédérale sur la protection des données (LPD ; cf. ci-dessous ch. 2.1)[1] sur l'élaboration de bases légales nécessaires aux organes fédéraux pour traiter des données personnelles sur des personnes physiques et de rappeler les principes de base de la protection des données, qui demeurent inchangés. La forme est résumée; le présent document se base sur une note détaillée de l'Office fédéral de la justice, OFJ, sur la révision totale de la loi sur la protection des données intitulée *Totalrevision des Datenschutzgesetzes: Übersicht zu den wichtigsten Änderungen für die Erarbeitung der Rechtsgrundlagen betreffend Datenbearbeitungen durch Bundesorgane* (ci-après: *"Note OFJ relative à la révision totale de la LPD"*), et y renvoie.

Comme le précédent guide, le présent document constitue un outil parmi d'autres qui s'adresse au légiste chargé d'élaborer des bases légales nécessaires aux organes fédéraux pour traiter des données personnelles sur des personnes physiques. Cet outil se concentre sur les éléments à prendre en compte lors de l'élaboration des bases légales susmentionnées. Il ne couvre pas tous les aspects de la protection des données. Il ne couvre pas, en particulier, des domaines très importants tels la sécurité des données, qui nécessitent, en particulier, l'adoption de mesures techniques et organisationnelles selon l'art. 3 de l'ordonnance sur la protection des données du 31 août 2022 (OPDo)[2] mais pas forcément l'élaboration de dispositions législatives spécifiques.

[1] La révision est entrée en vigueur le 1er septembre 2023.

[2] RS **235.11** - Ordonnance du 31 août 2022 sur la protection des données (OPDo) (admin.ch)

B) Liens avec le Guide de législation, la méthode de gestion de projet HERMES et l'analyse d'impact en matière de protection des données (AIPD)

Les besoins en matière de protection des données doivent être analysés dès la phase initiale d'un projet. Bien souvent, des bases légales doivent être modifiées ou créées. Le présent document présente les principaux enjeux à ce sujet et il complète à cet égard la démarche proposée au légiste dans le guide de législation[3].

En outre, la méthode HERMES de gestion de projet utilisée, en particulier, dans le domaine de l'informatique de la Confédération[4] prévoit l'élaboration d'un concept SIPD[5] (Sûreté de l'information et protection des données). Le présent document peut se révéler utile pour déterminer les exigences en matière de protection des données, pour évaluer les risques et pour déterminer les mesures à prendre en vue de l'élaboration de ce concept.

Une analyse d'impact en matière de protection des données (AIPD) est nécessaire lorsque le traitement envisagé est susceptible d'entraîner un risque élevé pour la personnalité ou les droits fondamentaux de la personne concernée (art. 22 LPD). Le Conseil fédéral a édicté les directives concernant l'examen préalable des risques et l'analyse d'impact relative à la protection des données personnelles en cas de traitement de données personnelles par l'administration fédérale (Directives AIPD) le 28 juin 2023[6]. D'autres outils pratiques sont mis à disposition sur le site de l'OFJ, tel, par exemple, l'instrument d'examen préalable des risques[7], le guide AIPD[8] et le document FAQ Droit de la protection des données[9].

---

[3] La version électronique du chapitre 14 du Guide de législation (OFJ, Guide de législation, 4ème éd., 2019) consacré à la protection des données personnelles a été actualisée en octobre 2023: Instruments de légistique (admin.ch).

[4] https://www.hermes.admin.ch/, Aperçu de la méthode (admin.ch) [5] Élaborer le concept SIPD (admin.ch).

[5] Élaborer le concept SIPD (admin.ch).

[6] FF **2023** 1882 - Directives du Conseil fédéral concernant l'examen préalable des risques et l'analyse d'impact relative à la protection des données personnelles en cas de traitement de données personnelles par l'administration fédérale (Directives AIPD).

[7] Instrument d'examen préalable des risques : https://www.bj.admin.ch/dam/bj/fr/data/staat/datenschutz/instrument-risikovorpruefung.xlsx.download.xlsx/instrument-risikovorpruefung-f.xlsx

[8] Guide AIPD : https://www.bj.admin.ch/dam/bj/fr/data/staat/datenschutz/dsfa-leitfaden.pdf.download.pdf/dsfa-leitfaden-f.pdf

[9] FAQ Droit de la protection des données, OFJ, septembre 2023

I Rappel du cadre constitutionnel

1.1 Droit à l'autodétermination informationnelle consacré à l'art. 13, al. 2 de la Constitution et à l'art. 8 de la Convention de sauvegarde des droits de l'homme et des libertés fondamentales

Le droit à l'autodétermination informationnelle consacré à l'art. 13, al. 2 Cst. (Cst[10]) et à l'art. 8 de la CEDH (CEDH[11]) confère à l'individu une forme de maîtrise sur ses propres données personnelles[12]. L'art. 13, al. 2, Cst. ne protège ainsi pas uniquement l'individu contre *"l'emploi abusif"* des données qui le concernent, comme le semble déclarer son libellé. Il couvre toute activité de traitement de données personnelles de l'État, par exemple la collecte, la conservation ou la communication de données personnelles[13]."*Dans le domaine de la protection des données, le droit à l'autodétermination en matière d'informations personnelles, consacré par la Constitution (art. 13, al. 2 Cst. et art. 8 CEDH), garantit que l'individu demeure en principe maître des données le concernant, indépendamment du degré de sensibilité effectif des informations en cause"*[14]. Il s'agit d'un droit fondamental. Les restrictions à ce droit doivent donc respecter les exigences constitutionnelles de base légale, d'intérêt public, de proportionnalité et de sauvegarde de l'essence des droits fondamentaux (art. 36 Cst.)[15]. Les restrictions graves aux droits fondamentaux doivent être prévues par une loi au sens formel (art. 36, al. 1, deuxième phrase Cst.). Les personnes chargées d'élaborer un acte normatif qui entraîne ou règle un traitement de données personnelles sont tenues de veiller au respect de ces exigences constitutionnelles et des exigences conventionnelles imposées par l'art. 8 CEDH[16] (ce même si la loi fédérale sur la protection des données ne s'applique pas comme lors de traitements de données par des organes publics cantonaux)[17].

1.2 Partage constitutionnel des compétences

La Constitution ne contient aucune disposition qui habilite expressément la Confédération à légiférer en matière de protection des données. La Confédération ne peut adopter des dispositions de protection des données que sur la base des dispositions constitutionnelles

---

[10] RS 101 - Constitution fédérale de la Confédération suisse du 18 avril 1999 (admin.ch)

[11] RS **0.101** - Convention du 4 novembre 1950 de sauvegarde des droits de l'homme et des libertés fondamentales (CEDH) (admin.ch)

[12] 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, Helbing Lichtenhahn, 2021, p. 44-63 [47-48] et la jurisprudence citée.

[13] ATF **128** II 259, consid. 3.2.

[14] ATF **140** I 381, consid. 4.1 (en français), ou ATF **138** II 346 consid. E 8.2 (en allemand); cf. également Note OFJ relative à la révision totale de la LPD, ch. 2.1.

[15] Au sujet de la restriction des droits fondamentaux, cf.: Guide de législation, n° 688.

[16] En relation avec la durée de conservation des données personnelles, cf. arrêt CourEDH *Catt c. Royaume-Uni* du 24 janvier 2019, requête n° 43514/15.

[17] Cf. Note OFJ relative à la révision totale de la LPD, ch. 2.1 ainsi que les références citées de doctrine et jurisprudence sur les droits de nature constitutionnelle qui découlent de l'art. 13, al. 2 Cst., en particulier le droit de connaître l'existence de données personnelles, de les consulter et de faire rectifier des données inexactes.

qui lui confèrent une compétence législative dans un domaine donné, par exemple celui des assurances sociales (assurance-vieillesse, survivants et invalidité, assurance-chômage, assurance maladie et accident). En revanche, lorsque la Constitution attribue à la Confédération la compétence de légiférer dans un certain domaine, le législateur fédéral peut être amené à adopter des dispositions de protection des données spécifiques, qui s'appliquent également aux autorités cantonales chargées d'exécuter le droit fédéral, par exemple en matière d'assurances sociales.

Il incombe aux cantons de légiférer sur la protection des données dans leurs domaines de compétences[18]. Les traitements de données effectués par des organes cantonaux (ou communaux) relèvent – sous réserve de règles contenues dans des lois fédérales spéciales – du droit cantonal, y compris lorsque les organes en question exécutent le droit fédéral ou ont obtenu les données au moyen d'un accès en ligne à une banque de données fédérale[19].

II Cadre légal, notions, principes

2.1 Remarques préliminaires

La loi fédérale sur la protection des données du 25 septembre 2020 (LPD), remplace la loi fédérale sur la protection des données de 1992 (aLPD ou loi de 1992)[20] pour mieux répondre aux défis liés aux nouvelles technologies en visant à améliorer la transparence des traitements de données[21] et en renforçant le droit constitutionnel à l'autodétermination informationnelle. La LPD reprend les notions et les principes qui ont fait leurs preuves. Elle ne crée pas de nouvelle compétence en faveur de la Confédération, si bien que les cantons restent souverains, sous réserve des dispositions fédérales matérielles sectorielles évoquées ci-dessus (cf. ch. 1.2).

---

[18] Echange de données personnelles entre autorités fédérales et autorités cantonales. Rapport du Conseil fédéral en exécution du postulat Lustenberger 07.3682 du 5 octobre 2007 "*Faciliter l'échange de données entre autorités fédérales et cantonales*" FF **2011** p. 624.

[19] Message concernant la loi fédérale sur la révision totale de la loi fédérale sur la protection des données et sur la modification d'autres lois fédérales du 15 septembre 2017, FF 2017 6565, p.6577 (ci-après: "Message concernant la révision totale de la LPD); cf. également Note OFJ relative à la révision totale de la loi sur la protection des données, ch. 4.5. ainsi que le rapport précité du Conseil fédéral en exécution du postulat Lustenberger, ch, 2.1, FF **2011** p. 624.

[20] Elle remplace aussi la loi du 28 septembre 2018 sur la protection des données Schengen, RS **235.3**, cf. ci-dessous note de bas de page n°22.

[21] Message concernant la révision totale de la LPD FF **2017** p. 6567, voir cependant : Bertil COTTIER, Transparence des traitements de données personnelles opérés par les organes fédéraux: un pas en avant, deux en arrière, RSDA 2021 p. 65 ss, 65) selon lequel: "*Le présent projet de loi vise à renforcer la protection des données, au travers notamment d'une amélioration de la transparence des traitements et du contrôle que les personnes concernées peuvent exercer sur leurs données." Autant dire qu'à l'entame de son message à la révision totale de la loi sur la protection des données, le Conseil fédéral exprime sans détours ses intentions: une des priorités de la nouvelle loi sera d'accroitre la visibilité des traitements de données personnelles. La révision de la loi fédérale sur la protection des données enfin sous toit, il y a lieu de se demander si cet objectif fondamental a réellement été atteint. C'est sans ambages que l'on répondra oui s'agissant des traitements opérés par des personnes privées ; et ce, en raison avant tout de l'ampleur du devoir d'information désormais à la charge du responsable du traitement. Pour ce qui concerne les traitements opérés par des organes fédéraux, la réponse est en revanche mitigée. Certes, des coups de projecteurs bienvenus ont été apportés ici ou là : intelligibilité des décisions automatisées, extension du droit d'accès et annonce des violations de la sécurité des données notamment. Ces avancées ponctuelles ne sauraient toutefois masquer un recul majeur: la révision a affaibli le devoir d'information des autorités fédérales".*

Le droit suisse doit remplir les exigences du développement de l'acquis Schengen, en particulier de la directive (UE) 2016/680 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales dans le cadre de l'acquis de Schengen[22].

En outre, les bases légales sectorielles en matière de protection des données devront également remplir les exigences de la Convention modernisée du Conseil de l'Europe sur la protection des données 108+[23], qui a été ratifiée par la Suisse le 7 septembre 2023 et qui entrera en vigueur lorsque 38 Etats parties l'auront ratifiée[24].

De plus, la Suisse bénéficie d'une décision d'adéquation de l'UE qui reconnaît la Suisse comme un Etat tiers ayant un niveau adéquat de protection des données pour échanger des données avec elle sans obstacle[25]. Il est dès lors important que la législation suisse en matière de protection des données, y compris le droit sectoriel, respecte le standard de protection des données du Règlement général sur la protection des données de l'Union européenne (règlement (UE) 2016/679, RGPD. La Commission européenne a ainsi confirmé dans son rapport du 15 janvier 2024 que le droit suisse en matière de protection des données répond toujours aux standards européens[26].

2.2 Champ d'application personnel et matériel

La LPD vise ainsi à protéger la personnalité et les droits fondamentaux des personnes physiques dont les données personnelles font l'objet d'un traitement (art. 1 LPD).

Le champ d'application de la LPD a été restreint aux données sur les personnes physiques. Comme dans l'aLPD, un catalogue d'exceptions à l'application de la LPD est prévu à l'art. 2 LPD et inclut, par exemple, les traitements de données personnelles effectués dans le cadre de procédures devant les tribunaux.

En revanche, le champ d'application de la LPD ne comprend plus les données sur les personnes morales. Le traitement des données personnelles sur les personnes morales est désormais réglé dans la loi sur l'organisation du gouvernement et de l'administration

---

[22] Le Parlement a divisé la proposition initiale de révision totale de la LPD du Conseil fédéral en deux étapes. Dans un premier temps, seule la directive UE 2016/680 relative à la protection des données en matière pénale a été mise en œuvre (voir, par exemple, le Rapport explicatif 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 dans le cadre de l'acquis de Schengen. La loi fédérale sur la protection des données personnelles dans le cadre de l'application de l'acquis de Schengen dans le domaine pénal (Loi sur la protection des données Schengen, LPDS) est entrée en vigueur le 1er mars 2019 pendant que le Parlement continuait d'examiner la révision totale de la LPD. La LPD abroge la LPDS, le contenu de cette dernière est repris dans la LPD.

[23] Protocole d'amendement à la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel du 10.10.2018, (STCE n° 223).

[24] La Suisse ratifie le Protocole d'amendement à la Convention 108 - Protection des données (coe.int), 31 Etats ont ratifié le protocole sumentionné jusqu'au 6 février 2024.

[25] Processus de décision d'adéquation, voir art. 45 RGPD.

[26] La Commission européenne a publié son rapport sur le niveau d'adéquation de la protection des données de plusieurs États tiers le 15 janvier 2024. Elle y reconnaît que la Suisse continue d'offrir un niveau de protection des données personnelles adéquat : L'UE confirme que la Suisse offre un niveau adéquat de protection des données (admin.ch).

(LOGA[27]), telle que modifiée par l'annexe 1/II de la LPD. En effet, les personnes morales peuvent se prévaloir de l'art. 13, al. 2 Cst. Cela signifie notamment que les organes fédéraux ne sont en droit de traiter ou de communiquer des données concernant des personnes morales que s'il existe une base légale suffisante. La révision totale de la LPD introduit dans la loi sur l'organisation du gouvernement et de l'administration plusieurs dispositions légales qui règlent la marche à suivre pour traiter des données concernant des personnes morales par les organes fédéraux (art. 57*r* ss LOGA). En outre, la disposition transitoire de l'art. 71 LPD devrait permettre d'éviter l'apparition de lacunes juridiques[28].

Si un organe fédéral envisage de traiter des données qui ne contiennent aucune information qui se rapporte à une personne physique identifiée ou identifiable, les exigences de la LPD ne sont pas applicables. Il tient compte, lors de son évaluation, du risque de mise en relation de données factuelles avec d'autres données ou de processus techniques susceptibles de créer un lien avec des personnes.

2.3 Notions

Les exigences en matière de restriction des droits fondamentaux et le principe de légalité (art. 5 Cst.) imposent aux organes fédéraux de disposer d'une base légale pour pouvoir traiter des données personnelles[29], que les données soient sensibles ou non.

Il s'agit de créer cette base légale dans les lois sectorielles. La LPD fixe les exigences que doivent remplir ces bases légales sectorielles (art. 34 et 36 LPD). Par rapport à la loi de 1992, elle modifie certaines notions comme celle des données sensibles, ou en introduit de nouvelles telles que, par exemple, les profilages[30].

2.3.1 Données personnelles

La notion de données personnelles demeure inchangée (art. 5, let. a LPD). Elle comprend toutes les informations concernant une personne physique identifiée ou identifiable. La notion demeure large, par exemple, une adresse IP (Internet Protocol, c'est-à-dire le numéro d'identification attribué à chaque machine accédant à internet) peut suffire dans certaines conditions pour être considéré comme une donnée personnelle[31].

---

[27] RS **172.010** - Loi du 21 mars 1997 sur l'organisation du gouvernement et de l'administration (LOGA)

[28] Cf. Note OFJ relative à la révision totale de la LPD, ch. 3 (en particulier ch. 3.2).

[29] À ce sujet cf. Note OFJ relative à la révision totale de la LPD, ch. 2. (en particulier le ch. 2.1).

[30] Voir, notamment, les commentaires suivants sur la LPD : Bruno BAERISWYL, Kurt PÄRLI, Dominika BLONSKI, Stämpflis Handkommentar SHK, Datenschutzgesetz (DSG), Bundesgesetz vom 25. September 2020 über den Datenschutz (DSG), 2. Auflage, 2023; Philippe MEIER, Sylvain MÉTILLE, Commentaire romand sur la loi fédérale sur la protection des données, Helbing Lichtenhahn, 2023; Yaniv BENHAMOU, Bertil COTTIER, Petit commentaire LPD, Loi sur la protection des données, Helbing Lichtenhahn, 2023; Adrian BIERI. Julian POWELL, Orell Füssli Kommentar (OFK) DSG Kommentar zum Schweizerischen Datenschutzgesetz mit weiteren Erlassen, 2023; David VASELLA, Gabor P. BLECHTA. Basler Kommentar (BSK) zum Datenschutzgesetz und Öffentlichkeitsgesetz, 4. Auflage, Basel 2024; Thomas STEINER, Anne-Sophie MORAND, Daniel HÜRLIMANN (Hrsg.), Onlinekommentar zum Bundesgesetz über den Datenschutz – Version: 25.08.2023: https://onlinekommentar.ch/de/kommentare/dsg43 (besucht am 12. Dezember 2023), DOI: 10.17176/20230825-103609-0.

[31] ATF **136** II 508, consid. 3 ; Philippe MEIER / Nicolas TSCHUMY Nicolas, *L'adresse IP : une donnée personnelle ? Ou quand la CJUE rejoint le TF !*, in : Jusletter 23 janvier 2017, n^os^ 22 ss.

Un organe fédéral n'est, en principe[32], en droit de traiter et de communiquer des données personnelles à des tiers que s'il existe une base légale (art. 5, al. 1, Cst. ; art. 34, al. 1, LPD).

2.3.2 Données sensibles

Le catalogue des données sensibles est élargi (art. 5, let. c LPD). Il inclut toutes les catégories de données considérées comme sensibles au sens de l'aLPD, c'est-à-dire les données personnelles sur les opinions ou activités religieuses, philosophiques, politiques ou syndicales, sur la santé, sur la sphère intime ou sur l'origine raciale, sur des poursuites ou sanctions pénales et administratives, sur des mesures d'aide sociale.

Le catalogue comprend désormais aussi les catégories suivantes[33]:

-les données sur l'origine ethnique ;

-les données génétiques ;

-les données biométriques identifiant une personne de manière univoque.

En principe une loi au sens formel doit prévoir le traitement de données sensibles (art. 34, al. 2, let. a LPD; cf. ci-dessous ch. 3.2.1).

2.3.3 Profilage

La LPD définit la notion de profilages comme une forme particulière de traitement automatisé des données personnelles qui consiste à utiliser des données pour évaluer de manière automatisée certains aspects personnels d'une personne physique (art. 5, let. f LPD). En utilisant des méthodes statistiques et mathématiques, en particulier des algorithmes, de nouvelles informations sur les individus peuvent être générées à partir d'une grande quantité de données, qui peuvent ne pas être très informatives en elles-mêmes. La notion de profilage remplace la notion de profils de la personnalité de la loi de 1992 mais s'en distingue. Alors qu'un profil de personnalité est le résultat d'une procédure de traitement, le profilage décrit une méthode de traitement des données[34], c'est-à-dire une évaluation automatisée de certains aspects d'une personne physique[35] .

Le Parlement a, en outre, introduit la notion de profilage à risque élevé (art. 5, let. g LPD). Ce type de profilage entraîne un risque élevé pour la personnalité parce qu'il conduit à un appariement de données, qui permet d'apprécier les caractéristiques essentielles de la

---

[32] A ce sujet cf. Note OFJ relative à la révision totale de la LPD, ch. 2.1 (en particulier *Ausnahmen vom Erfordernis der gesetzlichen Grundlage*).

[33] A ce sujet cf. Note OFJ relative à la révision totale de la LPD, ch. 2 (en particulier le ch. 2.2 ainsi que le ch. 2.2.1, let. a).

[34] A ce sujet cf. Note OFJ relative à la révision totale de la LPD, ch. 2.2.1, let. b.

[35] Le profilage représente ainsi une technique d'analyse et de prédiction du comportement humain. Elle est fondée sur l'exploitation de données par des modèles mathématiques appelés algorithmes, qui appliquent des techniques statistiques, d'analyse de données et de probabilité. Ces modèles visent à établir une corrélation entre, d'une part, certaines caractéristiques personnelles et factuelles (input) et, d'autre part, un état ou un comportement donné que l'on veut prédire, influencer ou même imposer (output), cf. Michael MONTAVON, Cyberadministration et protection des données, Étude théorique et pratique de la transition numérique en Suisse du point de vue de l'État, des citoyenne-s et des autorités de contrôle, Genève - Zurich - Bâle 2021, p. 639.

personnalité d'une personne physique[36]. Cette distinction n'a cependant guère de conséquences sur les organes fédéraux. La base légale qui prévoit des profilages (à risque élevé ou non) effectués par des organes fédéraux doit en principe être une loi au sens formel (art. 34, al. 2, let. b LPD; cf. ci-dessous ch. 3.2.2). Le traitement, y compris la communication de données basées sur le profilage (cf. ci-dessous ch. 3.2.4), devrait aussi être soumis à des exigences particulières[37].

2.3.4 Décision individuelle automatisée

La LPD définit la décision individuelle automatisée comme une décision prise exclusivement sur la base d'un traitement de données personnelles automatisé et qui a des effets juridiques pour la personne concernée ou l'affecte de manière significative (art. 21 LPD).

Cela signifie que l'évaluation d'une situation et la décision individuelle qui en découle sont réalisées par une machine ou un algorithme sans l'intervention d'une personne physique[38]. Dans ce cas de figure, la machine n'est pas seulement un outil ou une aide à la décision (voir ci-dessous ch. 2.3.5) [39].

Seules les décisions individuelles automatisées qui présentent une certaine complexité sont considérées comme telles (et non, par exemple, le contrôle de l'entrée dans un bâtiment sur la base d'une carte de légitimation)[40].

Le recours à la décision automatisée peut (mais ne doit pas nécessairement) constituer un cas prévu par l'art. 34, al. 2, let. c LPD (c'est-à-dire être considéré comme un mode de traitement susceptible de porter gravement atteinte aux droits fondamentaux de la personne concernée). Dans ce cas, une base légale au sens formel doit le prévoir.

2.3.5 Soutien automatisé à la prise de décision individuelle grâce à des systèmes d'algorithmes ("intelligence artificielle")

Le soutien automatisé à la prise de décision individuelle grâce à des systèmes d'algorithmes ("***intelligence artificielle***"[41]) n'est pas réglementé en tant que tel dans la LPD. Il n'y a pas de

---

[36] Sylvain MÉTILLE, *Le traitement des données personnelles sous l'angle de la (nouvelle) loi fédérale sur la protection des données du 25 septembre 2021*, tiré à part de la Semaine judiciaire 2021 II 1, p. 26.

[37] Au sujet de la problématique du traitement de données (pas forcément sensibles) basées sur des profilages, cf. Note OFJ relative à la révision totale de la LPD, ch. 2.2 (en particulier le ch. 2.2.1, let. b/dd*)*.

[38] Au sujet de la problématique de l'admissibilité ou non des décisions individuelles automatisées lorsque l'autorité dispose d'un pouvoir d'appréciation, cf. Note OFJ relative à la révision totale de la LPD, ch. 2.2 (en particulier le ch. 2.2.1, let. c/cc [voir en particulier, *Fallgruppe 1: Automatisierte Einzelentscheidungen*]).

[39] *Ibidem*.

[40] *Ibidem*.

[41] Le droit suisse ne définit pas ce qu'est l'intelligence artificielle. Au plan international, la tendance est plutôt d'utiliser la notion de « systèmes d'intelligence artificielle ». Ainsi, selon le projet de convention-cadre du Conseil d'Europe sur l'intelligence artificielle, les droits des l'homme, la démocratie et l'Etat de droit du 14 mars 2024, il s'agit « *d'un système informatique qui déduit, à partir des données qu'il reçoit et en fonction d'objectifs explicites ou implicites, comment générer des résultats tels que des prévisions, des contenus, des recommandations ou des décisions susceptibles d'influer sur des environnements matériels ou virtuels. Les différents systèmes d'intelligence artificielle varient dans leurs niveaux d'autonomie et d'adaptabilité après leur déploiement* ». Ce texte se base sur la définition révisée de « système d'intelligence artificielle » adoptée par l'OCDE le 8 novembre 2023 (cf. la Recommandation du Conseil sur l'intelligence artificielle). La définition correspond dans les grandes

décision individuelle automatisée au sens de l'art. 21 LPD lorsque cette dernière est préparée de manière automatisée, mais prise par un être humain[42]. Les questions juridiques évoquées ci-dessus dans le cas des décisions individuelles automatisées peuvent cependant se poser d'une manière analogue, lors de soutien automatisé à la prise de décision individuelle grâce à *"l'intelligence artificielle"*[43].

Dans le même sens que décrit précédemment, le recours à *"l'intelligence artificielle"* peut (mais ne doit pas nécessairement) constituer un cas prévu par l'art. 34, al. 2, let. c LPD (c'est-à-dire être considéré comme un mode de traitement susceptible de porter gravement atteinte aux droits fondamentaux de la personne concernée). Dans ce cas, une base légale au sens formel doit le prévoir.

2.3.6 Traitement de données

La définition du traitement de données au sens de l'art. 5, let. d LPD n'est matériellement pas modifiée, même si elle comprend désormais explicitement l'enregistrement et l'effacement[44].

2.3.7 Responsable du traitement

Le responsable du traitement au sens de l'art. 5, let. j LPD est la personne privée ou l'organe fédéral qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement de données personnelles, c'est-à-dire des facteurs et des risques qui sont pertinents en vertu de la LPD (par exemple, quelles données sont traitées à partir de quelles sources, pendant combien de temps et de quelle manière[45]).

Cette notion remplace celle de maître du fichier. Comme l'ancienne notion de maître du fichier, le responsable du traitement doit être précisément déterminé dans la loi sectorielle car il est responsable du respect des prescriptions en matière de protection des données et c'est auprès de lui que la personne concernée pourra exercer son droit d'accès, élément clé du droit de la protection des données[46].

L'art. 3 de la loi fédérale sur les systèmes d'information de la Confédération dans le domaine du sport[47] prévoit, par exemple que :

---

lignes à celle du projet de règlement de l'UE sur l'intelligence artificielle (COM [2021] 206 final). En l'absence de définition propre, on pourra s'inspirer de ces descriptions.

[42] Cf. Note OFJ relative à la révision totale de la LPD, ch. 2.2 (en particulier le ch. 2.2.1, let. c/cc [voir en particulier: *Fallgruppe 2: Unterstützender Einsatz von künstlicher Intelligenz*]).

[43] *Ibidem*.

[44] Message concernant la révision totale de la LPD, p. 6641.

[45] A ce sujet, cf. Note OFJ relative à la révision totale de la LPD, ch. 4 (en particulier le ch. 4.1).

[46] *L'obligation d'information est complétée par le droit d'accès. Le droit d'accès est un élément clé du droit de la protection des données car il permet à la personne concernée de faire valoir les droits que lui octroie la loi,* cf. Sylvain MÉTILLE, *Le traitement des données personnelles sous l'angle de la (nouvelle) loi fédérale sur la protection des données du 25 septembre 2021*, tiré à partir de la Semaine judiciaire 2021 II 1, p. p. 30.

[47] RS **415.1** - Loi fédérale du 19 juin 2015 sur les systèmes d'information de la Confédération dans le domaine du sport (LSIS) (admin.ch)

"L'OFSPO est responsable de la sécurité des systèmes d'information et de la légalité du traitement des données".

Si le responsable du traitement traite les données conjointement avec d'autres organes fédéraux ou cantonaux ou encore avec des personnes privées, le Conseil fédéral est chargé de régler les responsabilités et les procédures de contrôle dans une ordonnance (art. 33 LPD).

La LPD étend certaines obligations du responsable du traitement ou lui en impose de nouvelles (art. 19 à 24 LPD)[48], en particulier celle de procéder à une analyse d'impact lorsque le traitement de données envisagé est susceptible d'entraîner un risque élevé pour la personnalité ou les droits fondamentaux de la personne concernée[49].

2.3.8 Sous-traitant

Le sous-traitant au sens de l'art. 5, let. k LPD est la personne privée ou l'organe fédéral qui traite des données personnelles pour le compte du responsable du traitement.

Les organes fédéraux peuvent confier un traitement de données à un sous-traitant si la loi le prévoit ou en concluant un contrat (art. 9 LPD). Cela ne les dispense pas de l'obligation d'assumer leur responsabilité en vertu de la législation sur la protection des données[50].

La sous-traitance peut, par ailleurs, aussi concerner des services informatiques de traitement de données en nuages (cloud) qui comporte des risques particuliers[51] et qui implique notamment des garanties et des mesures techniques et organisationnelles.

2.3.9 Tiers

La notion de tiers n'est pas définie dans la LPD. Il s'agit d'une personne privée, d'un organe cantonal ou fédéral qui n'est ni le responsable du traitement ni le sous-traitant. Contrairement à la loi de 1992 (cf. art. 10*a* aLPD), le sous-traitant n'est plus considéré comme un tiers (art. 9 LPD *a contrario*)[52].

---

[48] A ce sujet, cf. Note OFJ relative à la révision totale de la LPD, ch. 1.2.

[49] A ce sujet, cf. Note OFJ relative à la révision totale de la LPD, ch. 4.3 ainsi que cf. ci-dessus introduction let. B et les directives du Conseil fédéral concernant l'examen préalable des risques et l'analyse d'impact relative à la protection des données personnelles en cas de traitement de données personnelles par l'administration fédérale (Directives AIPD) du 28 juin 2023, FF **2023** 1882.

[50] A ce sujet, cf. Note OFJ relative à la révision totale de la LPD, ch. 4 (en particulier le ch. 4.1).

[51] Cf. Sylvain MÉTILLE, Utilisation de l'informatique en nuage par l'administration publique, AJP/PJA 6/2019, p. 609s; voir aussi Cloud Computing, Datenschutzrechtliche Rahmenbedingungen am Beispiel des Katnons Zürich, in Künstliche Intelligenz und Datenschutz, Schulthess, 2021 p. 65 ss.

[52] Cf. Note OFJ relative à la révision totale de la LPD précitée, ch. 4 (en particulier le ch. 4.1).

2.3.10 Activité de traitement

La notion d'activité de traitement remplace dans la LPD (art. 12 LPD) celle de fichier prévue dans la loi de 1992 (art. 11*a* aLPD). Les organes fédéraux doivent tenir des registres des activités du traitement et les déclarer au Préposé fédéral à la protection des données et à la transparence (art. 12 LPD).

2.4 Principes

La LPD reprend pour l'essentiel les principes existants. Tout traitement de données personnelles par des personnes physiques doit respecter les principes généraux de protection des données (art. 6 à 8 LPD), c'est-à-dire être conforme aux principes de la licéité (art. 6, al. 1 LPD), de la bonne foi (art. 6, al. 2 et al. 4 LPD), de la proportionnalité (art. 6, al. 2 LPD), de la reconnaissabilité (art. 6, al. 3 LPD), de la finalité (art. 6, al. 3 LPD), de l'exactitude (art. 6, al. 5 LPD) et de la sécurité des données (art. 8 LPD)[53].

L'examen du respect du principe de licéité va s'effectuer le plus souvent en relation avec celui de l'exigence de la base légale qui permet aux organes fédéraux de pouvoir traiter des données personnelles.

Le principe de proportionnalité englobe le principe de minimisation selon lequel le responsable de traitement collecte et traite uniquement les données qui sont nécessaires au traitement**.** Les données collectées doivent être proportionnées par rapport aux besoins du traitement. Autrement dit, "*les informations enregistrées doivent être pertinentes et strictement nécessaires au regard de la finalité du fichier*[54]". Ce principe doit être pris en compte dès la conception du traitement par le responsable du traitement.

Le principe de finalité ne subit pas de modifications matérielles majeures[55] mais sa formulation s'aligne mieux sur celle de l'art. 5 de la Convention modernisée du Conseil de l'Europe sur la protection des données 108+ (et celle du RGPD). Selon l'art. 6, al. 3 LPD, les données ne peuvent être collectées que pour des finalités déterminées et reconnaissables pour la personne concernée et doivent être traitées ultérieurement de manière compatible avec ces finalités. L'art. 4 de la loi fédérale sur la surveillance de la correspondance par poste et télécommunication, LSCPT[56], tel que modifié par la LPD[57], prévoit, par exemple, que certains services et autorités désignés dans la disposition légale peuvent uniquement traiter des données *"qui leur sont nécessaires pour ordonner, autoriser et mettre en œuvre la surveillance".*

---

[53] A ce sujet, cf. Note OFJ relative à la révision totale de la LPD, ch. 2.1 (en particulier *Anforderungen an die Normdichte*).

[54] Cf. art. 5, let. c RGPD, voir aussi les cinq grand principes de protection des données selon la Commission nationale de l'informatique et des libertés en France, Quels sont les grands principes des règles de protection des données personnelles ? | Besoin d'aide | CNIL.

[55] Message concernant la révision totale de la LPD, p. 6645.

[56] RS **780.1** - Loi fédérale du 18 mars 2016 sur la surveillance de la correspondance par poste et télécommunication (LSCPT) (admin.ch)

[57] FF **2020** 7427 7468

La conservation des données doit, en particulier, respecter ces principes de proportionnalité et de finalité. Le législateur doit limiter la durée du traitement des données à ce qui est nécessaire pour l'accomplissement d'une tâche déterminée (et non à ce qui pourrait être utile au cas où) en fixant des délais de conservation[58].

Le message du Conseil fédéral part du principe selon lequel une finalité déterminée prévue par une loi est en principe reconnaissable pour la personne concernée[59]. Une loi peut ainsi modifier dans une certaine mesure la finalité initiale du traitement de données, Le respect du principe de la bonne foi est réservé.

L'art. 96d de la loi sur l'assurance-chômage[60] prévoit, par exemple que :

> *"Les organes d'exécution mentionnés à l'art. 76, al. 1, let. a et c, peuvent accéder en ligne au registre des habitants pour vérifier le domicile de la personne assurée, dans la mesure où le droit cantonal les y autorise".*

La LPD introduit, de plus, les principes de protection des données dès la conception[61] et par défaut (art. 7 LPD). Ces principes sont partiellement nouveaux (ils découlent en partie des principes existants de proportionnalité et de sécurité des données).

III Questions à se poser lors de la conception d'une base légale pour permettre à des organes fédéraux de traiter des données personnelles

3.1 Remarques préliminaires et exigences du principe de légalité

Après la phase initiale du projet, les questions préalables à se poser lors de la conception d'une base légale pour permettre à des organes fédéraux de traiter des données personnelles demeurent en partie analogues à celles que l'on se posait sous l'empire de la loi de 1992.

Il s'agit, en particulier, de se demander, si un traitement de données personnelles et/ou de données sensibles est envisagé, d'examiner la gravité possible de l'atteinte aux droits fondamentaux des personnes concernées et de déterminer la finalité des traitements de données, tout en gardant à l'esprit les exigences du principe de légalité (voir aussi ch. 2.3 ci-dessus).

Lorsqu'il ne s'agit pas de nouvelles tâches étatiques, c'est-à-dire qu'il existe déjà une base légale pour les traitements de données nécessaires à l'accomplissement de ces tâches, mais

---

[58] Thomas HELD, Markus BRÖNIMANN, in Orell Füssli Kommentar (OFK) DSG Kommentar zum Schweizerischen Datenschutzgesetz mit weiteren Erlassen, 2023, éd. Adrian BIERI; Julian POWELL, ad art. 34 n°9 -10 et la jurisprudence citée.

[59] Cf. Message concernant la révision totale de la LPD, p. 6645 : *"Lorsque la modification du but initial est prévue par la loi, requise par un changement législatif ou légitimée par un autre motif justificatif (par ex. le consentement de la personne concernée), le traitement ultérieur est aussi considéré comme compatible avec le but initial"*.

[60] RS **837.0** - Loi fédérale du 25 juin 1982 sur l'assurance-chômage obligatoire et l'indemnité en cas d'insolvabilité (Loi sur l'assurance-chômage, LACI) (admin.ch)

[61] Voir à ce sujet, Sylvain MÉTILLE, 9 novembre 2020, La notion de protection des données dès la conception – swissprivacy.law.

qu'un nouveau concept de traitement des données est envisagé, il est nécessaire, dans un premier temps, d'analyser la situation actuelle *("Ist")* et de la comparer avec la situation envisagée ("*Soll"*). Cette démarche permet de déterminer si cette situation crée des nouveaux traitements données et/ou présente de nouveaux risques pour les personnes concernées. La réponse à cette question oriente le légiste sur la question du niveau normatif et de la densité normative des bases légales à élaborer.

3.1.1 Exigences du principe de légalité

Le principe de légalité exige un degré suffisant de concrétisation des normes légales. Ces dernières doivent être formulées de manière suffisamment précise pour que les administrés puissent orienter leur comportement en fonction de ces normes et être en mesure d'évaluer les conséquences de leur comportement avec un degré suffisant de certitude[62].

La base légale qui prévoit un traitement de données personnelles par les organes fédéraux doit ainsi permettre à la personne concernée de reconnaître quel organe fédéral traite quelles catégories de données, dans quel but (qui, quoi, pourquoi) et, dans certains cas, quel est le mode de traitement, notamment en cas d'accès en ligne.

La base légale doit, en effet, également fournir des indications sur le mode de traitement, en particulier lorsque des moyens technologiques non reconnaissables pour l'administré sont utilisés et que le recours à ces moyens peut avoir un impact sur les droits fondamentaux[63]. Par exemple, s'il existe un risque de discrimination lié au traitement de données par un algorithme[64] ou un risque d'atteinte à la liberté personnelle du fait du recours à des outils de surveillance dans l'espace public. Plus l'atteinte aux droits fondamentaux peut être grave, plus la base légale doit être précise. A l'inverse, lorsque le traitement de données découle de manière inhérente de la tâche assumée par l'autorité, et que le risque d'atteinte aux droits fondamentaux est minime, par exemple lorsque l'autorité est chargée d'octroyer une aide financière, une base légale explicite pour le traitement de données personnelles n'est pas forcément indispensable et une éventuelle base légale spécifique pour la communication pourra être relativement générale.

3.1.2 Communication de données et principe de légalité

La communication de données doit en effet être prévue expressément dans une base légale (art. 36 LPD). Elle nécessite dès lors une base légale spécifique (cf. ci-dessous ch. 3.2.4) prévoyant qui a accès aux données, à qui les données peuvent, cas échéant, être communiquées et dans quel but, ainsi que le mode de communication et l'étendue du traitement dans les grandes lignes (qui, quoi, à qui, pourquoi, comment).

---

[62] ATF **146** I 11, 136 I 87 ; Jacques DUBEY, Petit commentaire Constitution, Art. 36 N 79.

[63] Monique COSSALI SAUVAIN, in Petit commentaire LPD, Loi sur la protection des données, éd. Yaniv BENHAMOU, Bertil COTTIER, Helbing Lichtenhahn, 2023, ad art. 34 n° 13.

[64] Frederik J. ZUIDERVEEN BORGESIUS., Discrimination, artificial intelligence and algorithmic decision-making, p. 13 ss et 36.

L'art. 20*b*, al. 1 de la loi fédérale sur les écoles polytechniques fédérales[65] prévoit, par exemple, que:

> *"Le Conseil des EPF, les EPF et les établissements de recherche peuvent au cas par cas, sur demande précise et écrite, indiquer à des organes de hautes écoles ou d'institutions de recherche ou d'encouragement de la recherche, suisses ou étrangères, qui sont chargés d'instruire et de sanctionner les manquements à la probité scientifique:*
>
> > *a. si les personnes relevant des EPF ont enfreint des règles relatives à l'intégrité scientifique et aux bonnes pratiques scientifiques ou s'il existe un soupçon fondé d'une telle infraction;*
> >
> > *b. quelles sanctions ont été prises à l'encontre des personnes concernées".*

L'art. 20*c* de cette loi prescrit l'information par écrit de la personne concernée.

3.1.3 Architecture informatique et principe de légalité

La question de savoir dans quelle mesure l'architecture d'un système d'information devait être décrite dans les bases légales s'est posée avec acuité, sous l'empire de la loi de 1992, en particulier pour les unités administratives qui utilisent des micros services en lieu et place des systèmes de silos.

On est en présence d'un accès en ligne lorsque plusieurs autorités exploitent le même système informatisé ou que des tiers par rapport au responsable du traitement ont accès selon le principe du self-service aux données. Dans ce cas de figure, le responsable du traitement demeure passif. Il ne sait pas forcément qu'une personne a eu accès à certaines données. La LPD ne distingue plus la notion de procédure d'appel visée à l'art 19, al. 3 aLPD[66]. En revanche, cette modification n'entraîne pas d'affaiblissement de la protection des données[67]. Il s'agit d'un mode de communication qui comme tel doit être prévu par la loi. L'accès en ligne selon le principe du self-service est particulièrement susceptible de porter gravement atteinte aux droits fondamentaux de la personne concernée, il doit être prévu dans une loi au sens formel en tout cas lorsqu'il porte sur des données sensibles ou des données basées sur des profilages. Il peut figurer dans une loi au sens matériel si le responsable du traitement donne un accès en ligne à des données non sensibles et que la probabilité d'atteinte grave aux droits fondamentaux est réduite. Le principe de finalité exige qu'un lien étroit soit établi entre l'accès en ligne et chaque tâche de l'autorité pour lesquelles il est requis. Par exemple, une autorité x a accès en ligne aux catégories de données y pour exécuter une tâche prévue à l'art. z de telle loi. Une autre autorité a accès en ligne aux catégories de données b pour accomplir une tâche c prévue à l'art. d de telle loi. Les bases légales nécessaires pour prévoir un accès en ligne seront d'autant plus précises que le risque d'atteinte aux droits fondamentaux est élevé. La gravité de l'atteinte doit être

---

[65] RS **414.110** - Loi fédérale du 4 octobre 1991 sur les écoles polytechniques fédérales (Loi sur les EPF) (admin.ch)

[66] Pour une approche critique de cette modification, voir Michael MONTAVON, L'abandon de la procédure d'appel en protection des données*, in:* LeGes 31 (2020) 2 p. 1-10.

[67] Message concernant la révision totale de la LPD, p. 6698.

examinée en tenant compte non seulement de la nature des données mais aussi et en particulier du but du traitement.

Lors de l'élaboration de la réglementation des traitements de données, l'accent est ainsi moins mis sur l'architecture informatique (technique) que sur *l'"architecture de traitement des données"*, à savoir les finalités et la logique du traitement ainsi que les flux de données et les accès en ligne aux données (qui a accès à quelles données [68]). Lorsque des données sont traitées pour l'accomplissement de plusieurs tâches légales, la réglementation correspondante doit être différenciée en fonction de ces tâches, pour montrer qui peut effectuer tel ou tel traitement pour accomplir telle ou telle tâche légale et quelles sont les modalités de ce traitement.

En cas de pluralité de tâches légales, il est important que la loi distingue clairement pour quelle tâche légale quelles données personnelles peuvent être traitées et par qui. Cela est d'autant plus important que dans les systèmes modernes, les *"solutions en silo"* sont remplacées par des solutions structurées différemment (comme mentionné ci-dessus par exemple des *"microservices")* et que la loi doit rester neutre sur le plan technologique. C'est pourquoi il est nécessaire de réglementer le traitement des données personnelles en fonction des tâches à accomplir.

L'art. 9, al. 1 de la loi fédérale sur le dossier électronique du patient[69] prévoit, par exemple, que :

> *"Les professionnels de la santé ne peuvent accéder aux données des patients que dans la mesure où ceux-ci leur ont accordé un droit d'accès".*

3.1.4 Devoir d'informer et principe de légalité

La LPD continue, en outre, de prévoir un devoir d'informer qui renforce la transparence des traitements. L'organe fédéral responsable du traitement est cependant délié du devoir d'informer lorsque le traitement est prévu par la loi[70]. Cette dernière doit dès lors prévoir les informations nécessaires à la mise en œuvre des droits de la personne concernée et garantir la transparence du traitement[71].

---

[68] A ce sujet, cf. Note OFJ relative à la révision totale de la LPD, ch. 2.1.

[69] RS **816.1** - Loi fédérale du 19 juin 2015 sur le dossier électronique du patient (LDEP) (admin.ch)

[70] Voir à ce sujet, Bertil COTTIER, Transparence des traitements de données personnelles opérés par les organes fédéraux: un pas en avant, deux en arrière, RSDA 2021 p. 65 ss, 70 qui compare les exemptions restrictives au devoir d'information selon l'art. 18a aLPD et,l'exemption large prévue à l'art. 20, al. 1, let. b nLPD; il en tire la conclusion suivante (p.72):

"Reste que cette regrettable exemption n'est en soi pas contraire au droit international supérieur: (...), la convention 108 modernisée la prévoit déjà, au motif implicite que „Nul n'est censé ignorer la loi". Cela dit, comme le souligne la doctrine, cet adage permet certes „de considérer que les citoyens sont déjà informés, mais cela n'est valable qu'à la condition que la loi en question soit suffisamment précise et apporte les renseignements nécessaires pour assurer une information loyale de personnes concernées".

[71] Message concernant la révision totale de la LPD, p. 6669 et 6671 ; voir aussi Claudius ETTLINGER, Die Informationspflicht gemäss neuem Datenschutzgesetz, in: Jusletter IT 16. Dezember 2021.

Une disposition légale telle que l'art. 7*a*, al. 3 de la loi sur le système d'information commun aux domaines des étrangers et de l'asile[72] prévoyant de manière générale que :

> *" Pour accomplir leurs tâches légales, les autorités et services suivants sont habilités à traiter les données biométriques dans le système d'information"*
>
> *(…)*
>
> *g. le bureau SIRENE de fedpol";*

ne serait probablement plus considérée comme offrant une information suffisante à la personne concernée.

La collaboration avec les informaticiens responsables de la mise en œuvre technique des traitements de données demeure ainsi essentielle pour saisir, dans une certaine mesure, les potentialités informatiques d'un projet de traitement de données. Le responsable du traitement doit d'ailleurs prendre, dès la conception du traitement, des mesures techniques et organisationnelles appropriées afin que le traitement respecte les principes relatifs à la protection des données et offre les garanties nécessaires afin de protéger les droits de la personne concernée[73].

A la suite de cette démarche, deux questions doivent, en particulier, être abordées lors de la conception d'une réglementation permettant à des organes fédéraux de traiter des données personnelles : celle du niveau normatif et celle de la densité normative des dispositions envisagées. Les réponses à ces questions dépendent des spécificités de la matière à régler. Elles ne sont ni schématiques ni ne devraient entraîner une règlementation disproportionnée.

3.1.5 Systèmes de gestion des affaires

L'art. 57*h* de la loi sur l'organisation du gouvernement et de l'administration, LOGA[74], tel que modifié par la LPD[75] prévoit la base légale permettant aux unités de l'administration fédérale de gérer des systèmes électroniques pour assurer le bon déroulement de leurs processus opérationnels et pour gérer des documents. Elles peuvent donner à d'autres autorités fédérales et à des unités qui sont extérieures à l'administration fédérale (services cantonaux par exemple) un accès de manière restreinte à leurs systèmes de gestion des affaires dans la mesure où cet accès est nécessaire au bon déroulement de leurs processus de travail (par exemple pour des consultations des offices).

L'ordonnance sur la gestion électronique des affaires dans l'administration fédérale, l'ordonnance GEVER[76], concrétise le but et le contenu des systèmes de gestion électronique des affaires. Elle prévoit en principe l'utilisation de GEVER standardisé mais permet

---

[72] RS **142.51** - Loi fédérale du 20 juin 2003 sur le système d'information commun aux domaines des étrangers et de l'asile (LDEA) (admin.ch)

[73] Art. 7 LPD, cf. Sylvain MÉTILLE, La notion de protection des données dès la conception, 9 novembre 2020 in www.swissprivacy.law/26.

[74] RS **172.010** - Loi du 21 mars 1997 sur l'organisation du gouvernement et de l'administration (LOGA)

[75] FF **2020** 7437

[76] RS **172.010.441** - Ordonnance du 3 avril 2019 sur la gestion électronique des affaires dans l'administration fédérale (Ordonnance GEVER)

également à certaines conditions des systèmes de gestion des affaires non standardisés (art. 3).

Lorsqu'on est en présence d'un système de gestion des affaires, on peut renoncer à édicter de nouvelles règles dans la mesure où le traitement des données peut se fonder sur la LOGA et sur l'ordonnance GEVER. Cela présuppose que l'ensemble de cette règlementation générale à laquelle s'ajoutent d'éventuelles dispositions sectorielles soient suffisantes pour que le traitement de données soit reconnaissable pour la personne concernée.

3.1.6 Projets pilotes

La LPD continue de prévoir la possibilité d'effectuer des projets pilotes, pour lesquels les exigences du principe de légalité sont assouplies[77].

3.2 Niveau normatif (loi au sens formel ou réglementation dans une ordonnance) et densité normative

Le risque d'atteinte aux droits fondamentaux a des conséquences sur la question du niveau normatif de la réglementation envisagée (loi au sens formel ou réglementation dans une ordonnance), ainsi que sur la densité normative. Ces deux questions sont ainsi à traiter ensemble pour le traitement et pour la communication de données personnelles, qui constitue une forme particulière de traitement.

3.2.1 Traitement de données sensibles

Selon l'art. 34, al. 2, let. a LPD, une base légale au sens formel doit prévoir le traitement de données sensibles au sens de l'art. 5, let. c, ch. 1 à 6 LPD (cf. ci-dessus ch. 2.3.2). En vertu du principe de légalité et pour garantir la transparence du traitement des données vis-à-vis de la personne concernée, la loi au sens formel doit nommer les catégories de données sensibles traitées, énumérées à l'art. 5, let. c, ch. 1 à 6 LPD. Le principe de proportionnalité impose de ne traiter que les catégories de données sensibles qui sont indispensables à l'exécution d'une tâche légale. Il s'agit donc de créer, dans la mesure du possible, des sous-catégories des catégories énumérées à l'art. 5, let. c, ch. 1 à 6 LPD, par exemple, dans le domaine des données sur la santé, de préciser que seules des données sur les cancers sont traitées[78], (cf. art. 3 de la loi fédérale sur l'enregistrement des maladies oncologiques[79]).

Quant à la question de la densité normative, plus les risques d'atteintes à la personnalité ou aux droits fondamentaux sont élevés, plus le degré de précision de la disposition légale doit être élevé et la finalité du traitement définie de manière précise et reconnaissable pour la personne concernée.

---

[77] Art. 35 LPD, à ce sujet, cf. Note OFJ relative à la révision totale de la LPD, ch. 2.1.

[78] A ce sujet, cf. Note OFJ relative à la révision totale de la LPD, ch. 2.2 (en particulier le ch. 2.2.1, let. a).

[79] RS **818.33** - Loi fédérale du 18 mars 2016 sur l'enregistrement des maladies oncologiques (LEMO) (admin.ch)

Les prescriptions décrites ci-dessus correspondent au droit antérieur . À l'art. 34, al. 3 LPD le législateur a, cependant, innové en prévoyant d'habiliter le Conseil fédéral à adopter une base légale au sens matériel prévoyant le traitement de données sensibles lorsque deux conditions cumulatives sont remplies :

-Le traitement doit être indispensable à l'accomplissement d'une tâche légale définie dans une loi au sens formel. La tâche doit être expressément définie dans la loi au sens formel et son étendue reconnaissable pour la personne concernée[80], et;

-La finalité du traitement ne présente pas de risques particuliers pour les droits fondamentaux de la personne concernée, notamment pour le respect de sa vie privée (comparer les art. 13 et 36, al. 1 Cst.; cf. ci-dessus ch. 1.1). Il s'agit, en outre, aussi de vérifier que le mode de traitement des données ne risque pas de porter une atteinte grave aux droits fondamentaux (cf. art. 34, al. 2, let. c LPD).

Ce n'est que si toutes ces conditions sont remplies qu'un recours à une réglementation dans une ordonnance est envisageable au sens de l'art. 34, al. 3 LPD.

3.2.2 Profilages (art. 34, al. 2, let. b LPD)

Les considérations formulées ci-dessus s'appliquent aux profilages. Le Conseil fédéral a estimé que l'exigence du niveau de la base légale pour le profilage doit être la même que celle pour le traitement de données sensibles[81]. La règle est donc que les organes fédéraux ne peuvent effectuer des profilages que si une loi au sens formel le prévoit. En ce qui concerne l'examen du respect du principe de proportionnalité, il est nécessaire, notamment, de se demander si d'autres possibilités de traitement de données qui permettraient de mieux protéger la personnalité des personnes concernées ne pourraient entrer en ligne de compte[82].

L'exigence de la base légale formelle n'est pas absolue ; l'art. 34, al. 3 LPD, commenté ci-dessus (cf. ch. 3.2.1) en relation avec le traitement des données sensibles, s'applique aussi aux profilages.

La base légale doit être suffisamment précise. Cela implique que la base légale prévoie explicitement le profilage au sens de l'art. 5, let. f LPD ou le décrive de manière adéquate. Elle doit au moins indiquer la finalité du profilage et les catégories de données utilisées dans le profilage. La personne concernée devrait également pouvoir reconnaître les caractéristiques de sa personne qui sont évaluées par le profilage. Le droit à l'autodétermination informationnelle s'applique ; la personne concernée par un profilage individualisé doit pouvoir exercer son droit d'accès et recevoir les informations des organes fédéraux qui lui permettent de comprendre la logique du profilage dont elle fait l'objet. Les organes fédéraux sont, de plus, tenus de prendre des mesures techniques et

[80] A ce sujet, cf. Note OFJ relative à la révision totale de la LPD, ch. 2.2 (en particulier le ch. 2.2.1, let. a).précitée.

[81] Message concernant la révision totale de la LPD, p. 6694 ss.

[82] A ce sujet, cf. Note OFJ relative à la révision totale de la LPD, ch. 2.2 (en particulier le ch. 2.2.1, let. b/dd).

organisationnelles pour minimiser le risque d'erreur[83], de violation du principe de l'interdiction de discrimination[84] ou du principe de l'interdiction de l'arbitraire.

L'art. 21*c*, al. 1, let. b, et al. 1[bis] de la loi fédérale sur l'aviation[85] tel que modifié par la LPD[86] prévoit, par exemple, que :

> "*les données suivantes relatives à des événements liés à la sûreté et aux individus potentiellement dangereux impliqués dans ces événements sont traitées dans le système d'information :*
>
> *(…)*
>
> *b. données personnelles nécessaires pour évaluer la menace pesant sur le trafic aérien commercial international, y compris les données sensibles, comme des informations sur l'état de santé, les condamnations ou les procédures pénales ou administratives en cours et sur l'appartenance à des groupes criminels ou terroristes";*

Il habilite, à son alinéa 1[bis,] Fedpol : "*à faire du profilage, (...) au sens de la loi fédérale du 25 septembre 2020 sur la protection des données pour évaluer la menace que représentent les personnes visées à l'al. 1".*

3.2.3 Risque d'atteinte grave aux droits fondamentaux de par la finalité ou le mode de traitement envisagé (art. 34, al. 2, let. c LPD)

La LPD rappelle expressément qu'une base légale au sens formel est exigée lorsque la finalité du traitement de données personnelles ou le mode de traitement peut porter gravement atteinte aux droits fondamentaux de la personne concernée (art. 36, al. 1 Cst.), indépendamment de la question de savoir si un traitement de données sensibles ou un profilage sont envisagés. Un risque d'atteinte grave peut résulter de la finalité du traitement envisagé (par exemple d'évaluer la dangerosité d'une personne[87)]. Il peut aussi résulter du mode de traitement envisagé, en particulier en cas de décision individuelle automatisée et lors de recours à l'"*intelligence artificielle"* sans décision individuelle automatisée. Une taxation fiscale entièrement automatisée constituerait un exemple de décision automatisée. En revanche, si la taxation est faite par une personne physique mais que le taxateur utilise un algorithme qui lui signale d'éventuelles incohérences dans la déclaration fiscale, il s'agirait de recours à l'intelligence artificielle sans décision automatisée.

---

[83] En application du principe d'exactitude (cf. art. 6 al. 5 LPD de 2020), le responsable du traitement qui procède à des activités de profilage doit s'assurer que les données qu'il utilise sont exactes par rapport aux finalités poursuivies et que les conclusions rendues à l'issue du profilage sont suffisamment fiables. Dans la mesure où les activités de profilage impliquent nécessairement un certain taux d'erreur, le responsable du traitement doit prendre les mesures appropriées afin d'écarter les facteurs d'inexactitudes tant des données utilisées que des prédications établies, cf. (MICHAEL MONTAVON, Cyberadministration et protection des données, Étude théorique et pratique de la transition numérique en Suisse du point de vue de l'État, des citoyen-ne-s et des autorités de contrôle, Genève - Zurich - Bâle 2021, p. 647).

[84] A ce sujet, cf. Note OFJ relative à la révision totale de la LPD, ch. 2.2 (en particulier le ch. 2.2.1, let. b/dd).

[85] RS **748.0** - Loi fédérale du 21 décembre 1948 sur l'aviation (LA) (admin.ch)

[86] FF **2020** 7468

[87] Message concernant la révision totale de la LPD, p. 6695.

Dans certaines circonstances, les décisions individuelles automatisées peuvent impliquer une atteinte grave aux droits fondamentaux de la personne concernée au sens l'art. 34, al. 2, let. c LPD, et doivent de ce fait être prévues dans une loi au sens formel. Elles peuvent également être considérées comme des questions importantes relatives à l'organisation et à la procédure des autorités fédérales, pour lesquelles une base légale en droit formel est requise selon l'art. 164, al. 1, let. g Cst[88]. La base légale doit prévoir expressément la décision individuelle automatisée ou la décrire de manière adéquate. La logique sur laquelle la décision automatisée repose doit être reconnaissable dans les grandes lignes pour la personne concernée[89].

Le recours à l'*"intelligence artificielle*" par l'administration pour préparer des décisions ne fait pas actuellement l'objet d'une réglementation spécifique[90]. Sur le plan fédéral, le Conseil fédéral a adopté le 25 novembre 2020 les lignes directrices *"Intelligence artificielle"*[91]. Ces dernières placent, en particulier, l'être humain au cœur des préoccupations et rappellent le cadre juridique du respect des droits fondamentaux, sans fournir de critères qui pourraient être mis en œuvre dans la législation[92].

3.2.4 Communication de données personnelles y compris l'accès à des données personnelles

La communication de données personnelles constitue un traitement de données personnelles au sens de l'art. 5, let. d LPD. La communication de données personnelles est une forme particulièrement sensible du traitement des données. Elle consiste à transmettre ou à rendre accessible des données (art. 5, let. e LPD) et est régie par l'art. 36 LPD.

Selon cette disposition, les organes fédéraux continuent d'avoir besoin d'une base légale spécifique qui prévoie la communication des données (cf. art. 19 aLPD et art. 36 LPD). Autrement dit, une disposition légale qui les habiliterait de manière générale à traiter des données ne serait pas suffisante[93].

Avant d'élaborer une base légale relative à la communication de données personnelles sensibles ou de profilages par un organe fédéral, le légiste détermine dans quelle mesure la communication de données porte atteinte à la personnalité de la personne concernée en tenant compte, notamment, de la nature des données transmises, de la finalité de la

---

[88] A ce sujet, cf. Note OFJ relative à la révision totale de la LPD, ch. 2.2 (en particulier le ch. 2.2.1, let. c).

[89] *Ibidem*.

[90] A ce sujet, cf.: Nadja BRAUN BINDER ; Thomas BURRI ;Melinda Florina LOHMANN , Monika SIMMLER, Florent THOUVENIN, Kerstin,Noëlle VOKINGER, *Künstliche Intelligenz: Handlungsbedarf im Schweizer Recht*, in: Jusletter, 28 juin 2021. Ces auteurs relèvent que la Commission européenne a présenté une proposition pour un règlement sur la réglementation de l'IA le 21 avril 2021.

[91] Conseil fédéral, *"Intelligence artificielle" - lignes directrices pour la Confédération, Cadre d'orientation en matière d'IA dans l'administration fédérale*, du 25 novembre 2020.

[92] Le recours à l'"*intelligence artificielle*" par l'administration a, en revanche, fait l'objet d'une analyse détaillée des défis juridiques et éthiques dans l'étude *"Einsatz Künstlicher Intelligenz in der Verwaltung" d*u 28 février 2021 commandée par le Canton de Zurich, *Cette étude traite de la question du niveau normatif ainsi que celle de la densité normative Staats*kanzlei Kanton Zurich, *Einsatz Künstlicher Intelligenz in der Verwaltung: rechtliche und ethische Fragen - Schlussbericht vom 28. Februar 2021 zum Vorprojekt IP6.4*, 28 février 2021, consultable à l'adresse suivante: https://www.zh.ch/de/news-uebersicht/medienmitteilungen/2021/04/kuenstliche-intelligenz-in-der-verwaltung-braucht-klare-leitlini.html (dernier accès le 12.10.2021).

[93] A ce sujet, cf. Note OFJ relative à la révision totale de la LPD, ch. 2.1.

communication et du cercle des destinataires ainsi que du mode de leur transmission. Il veille tout au long de sa démarche au respect du principe de proportionnalité (cf. ci-dessus ch. 2.4).

3.2.4.1 Risque d'atteinte à la personnalité et aux droits fondamentaux

Les exigences de base légale selon la gravité du risque d'atteinte à la personnalité et aux droits fondamentaux de la personne concernée sont largement les mêmes que pour les autres formes de traitement de données. L'art. 36, al. 1 LPD renvoie à ce sujet à l'art. 34, al. 1 à 3 LPD.

La communication de données sensibles est en principe à prévoir dans une loi au sens formel de même que celle de données basées sur un profilage. L'exception prévue à l'art. 34, al. 3 LPD s'applique (cf. ci-dessus ch. 3.2.1 in fine et ch. 3.2.2 in fine).

3.2.4.2 Reconnaissabilité et finalité de la communication

La communication doit être reconnaissable pour la personne concernée. Cette dernière doit être en mesure de savoir à qui ses données peuvent être transmises et dans quel but. La finalité de la communication doit, en outre, être compatible avec la finalité de la collecte des données (art. 6, al. 3 LPD). Une loi peut prévoir une finalité de la communication différente de celle initiale de la collecte de données. Le respect du principe de la bonne foi est réservé (comparer ch. 2.4 ci-dessus).

Lorsque la finalité de la communication diffère de celle de la collecte, il peut être important de modifier les deux lois, celle qui prévoit la collecte initiale et celle qui prévoit l'utilisation postérieure des données à d'autres fins, afin que la communication de données demeure reconnaissable pour la personne concernée. L'art. 50*a* de la loi sur l'assurance-vieillesse et survivants, (LAVS)[94]prévoit par exemple à son alinéa 2 que :

> *" Les données nécessaires à la lutte contre le travail au noir peuvent être communiquées conformément aux art. 11 et 12 de la loi du 17 juin 2005 sur le travail au noir "*.

La collaboration des autorités cantonales ou fédérales et des organisations privées chargées de l'application de la législation relative aux assurances sociales avec les organes de contrôle cantonaux prévus par la loi fédérale concernant des mesures en matière de lutte contre le travail au noir (Loi sur le travail au noir, LTN)[95] ainsi que la communication de données, notamment par les caisses de compensation AVS, est réglée de manière plus détaillée dans la loi sur le travail au noir.

---

[94] RS **831.10** - Loi fédérale du 20 décembre 1946 sur l'assurance-vieillesse et survivants (LAVS) (admin.ch)

[95] RS **822.41** - Loi fédérale du 17 juin 2005 concernant des mesures en matière de lutte contre le travail au noir (Loi sur le travail au noir, LTN) (admin.ch)

3.2.4.3 Mode de communication

On peut distinguer quatre modes de communication : la communication obligatoire (d'office ou sur demande), la communication spontanée, la communication sur demande (selon la libre appréciation de l'autorité requise), et l'accès en ligne (selon le principe du self-service)[96].

Le mode de communication retenu doit être conforme au principe de proportionnalité. Ainsi, lorsque la communication sur demande suffit à permettre au destinataire d'accomplir ses tâches légales, on ne prévoit pas de mode de communication plus large, comme par exemple un accès en ligne selon le principe du self-service.

Les dispositions légales doivent montrer de quel mode de communication il s'agit. Autrement dit, le légiste continue de devoir distinguer ces modes de communication dans les dispositions légales par des formules appropriées telles que :

> *-"l'autorité est tenue de transmettre d'office (...)" ;*
>
> *-"l'autorité peut signaler spontanément (...)";*
>
> *-"l'autorité peut communiquer dans des cas particuliers et sur demande écrite et motivée (...)".*
>
> *-"l'autorité peut octroyer un accès en ligne (ou ... peut accéder en ligne)"*

L'exigence d'une base légale expresse[97] a été abandonnée (comme souligné ci-dessus au ch. 3.1.3) pour la procédure d'appel, c'est-à-dire pour une procédure automatisée par laquelle le destinataire des données peut obtenir les données personnelles sans que l'organe fédéral responsable du traitement n'ait à les communiquer ni même ne s'aperçoive que les données ont été obtenues (principe du self-service). Cette modification législative entraîne cependant peu de changements matériels dans la mesure où la volonté du législateur est de maintenir la protection conférée par le système antérieurement en vigueur. L'accès en ligne constitue d'ailleurs un mode de communication qui doit continuer de figurer dans une loi au sens formel chaque fois qu'il est susceptible de porter gravement atteinte aux droits fondamentaux de la personne concernée (art. 34, al. 2, let. b LPD.), c'est-à-dire notamment et par définition, chaque fois qu'il porte sur des données sensibles ou des profilages. Dans les autres cas, ce mode de communication figure au moins dans l'ordonnance, à l'instar des autres modes de communication, pour respecter le principe de légalité et pour des raisons de transparence. Il s'agit, autrement dit, d'indiquer dans la disposition de la loi ou de l'ordonnance qu'il s'agit d'un accès en libre-service tandis que le responsable du traitement reste passif par des formules telles que "*permet l'accès en ligne*". Il s'agit également de distinguer dans la disposition légale s'il s'agit d'un "*accès"* complet aux données ou d'un *"accès à un index"*[98]*.*

---

[96] A ce sujet, cf. Guide de législation, n^os^ 829 ss ; ainsi que Note OFJ relative à la révision totale de la LPD, ch. 2.2 (en particulier le ch. 2.2.2), voir aussi Camille DUBOIS, (2012) : Recommandations pour la rédaction de dispositions légales réglant l'échange de données personnelles entre autorités, in : LeGes 23 (2012) 3, p. 389–396.

[97] A ce sujet, cf. Note OFJ relative à la révision totale de la LPD, ch. 2.2 (en particulier le ch. 2.2.2).

[98] *Ibidem*.

Le principe de proportionnalité doit également être respecté. En d'autres termes, cela signifie que seules les données nécessaires à l'accomplissement de leurs tâches légales peuvent être communiquées aux destinataires.

3.2.4.4 Densité normative et contenu minimum de la loi

Comme pour le traitement de données, la densité normative des dispositions dépend du risque d'atteinte à la personnalité de la personne concernée et aux droits fondamentaux. Il ressort de ce qui précède que la loi doit régler les points suivants :

-la ou les autorités responsables de la communication des données ;

-la finalité de la communication des données ;

-les catégories de données concernées, y compris les profilages ;

-les modes de communication des données ;

-le ou les destinataires[99].

3.2.5 Communication à l'étranger

La communication transfrontalière des données a subi certains changements : le principe est que le Conseil fédéral a constaté que l'État vers lequel les données sont communiquées offre un niveau de protection adéquat (art. 16, al. 1 LPD) dans sa législation et dans la mise en oeuvre de cette dernière. Dans ce cas, les données peuvent être communiquées sans autres formalités. En l'absence d'une telle constatation, les données ne peuvent être transférées à l'étranger que moyennant des garanties additionnelles (art. 16, al. 2 et 3 LPD). L'art. 17 LPD énumère les situations dans lesquelles il est permis de déroger à l'art. 16 al. 2 et 3 LPD et de transférer des données sans garanties additionnelles vers un Etat n'offrant pas un niveau de protection adéquat.

Selon l'art. 16, al. 1 LPD, des données personnelles ne peuvent en principe être communiquées à l'étranger que si la législation de l'État concerné garantit un niveau de protection adéquat ou qu'un organisme international garantit ce niveau de protection adéquat des données.

Le Conseil fédéral est chargé de déterminer quels États ou organismes internationaux assurent un tel niveau de protection. Les critères d'évaluation du niveau de protection adéquat des données personnelles d'un État étranger ou d'un organisme international sont fixés à l'art. 8 OPDo. Une liste des États étrangers qui assurent de niveau de protection adéquat figure en annexe à cette nouvelle ordonnance[100].

Des données personnelles peuvent être communiquées à un État qui ne figure pas sur la liste du Conseil fédéral si un niveau de protection approprié des données est garanti par

---

[99] Guide de législation, n° 833.

[100] A ce sujet, cf. Note OFJ relative à la révision totale de la LPD, ch. 4.2.

d'autres instruments au sens de l'art. 16, al. 2 LPD. Il s'agit notamment de traités internationaux ou de clauses contractuelles (art. 16, al. 2, let. a, b et d LPD).

Lors de la conclusion de traités internationaux, il est donc important de veiller à ce qu'un niveau de protection des données adéquat soit garanti à l'étranger. Le respect des principes de protection des données, des droits des personnes concernées (tel, notamment, le droit d'accès aux données), des voies de droit, des exigences relatives aux communications ultérieures et un contrôle indépendant de la protection des données sont essentiels.

L'art. 9 du Traité d'entraide judiciaire que la Suisse a conclu avec l'Indonésie[101] entré en vigueur le 14 septembre 2021 précise, notamment que (la citation est incomplète) :

*"1. Les données à caractère personnel qui sont transmises sur la base du présent Traité ne peuvent être utilisées qu'aux fins pour lesquelles elles ont été transmises **;** leur utilisation est soumise aux conditions formulées par l'État qui les a transmises.*

2. Les conditions suivantes s'appliquent à la transmission et à l'utilisation des données à caractère personnel qui ont été transmises dans le cadre d'une demande d'entraide au titre du présent Traité :

> *a. seules des données en rapport avec la demande peuvent être transmises à l'autorité compétente de l'État requérant ;*
>
> *b. sur demande, la Partie contractante qui a reçu les données informe l'État qui les a transmises de l'utilisation qui en a été faite et des résultats obtenus ;*
>
> *c. si l'État qui a transmis les données constate que des données erronées ou qui n'auraient pas dû être transmises l'ont été, celui-ci en informe immédiatement l'État qui les a reçues ; ce dernier corrige sans délai les erreurs éventuelles ou détruit les données reçues ;*
>
> *d. les Parties contractantes conservent sous une forme facilement accessible les documents et enregistrements concernant la transmission et la réception des données ;*
>
> *e. la transmission subséquente de données à caractère personnel est uniquement autorisée si elle est conforme au droit interne et que l'État qui les a transmises a donné au préalable son consentement ;*
>
> *f. les données transmises qui ne sont plus nécessaires aux fins prévues par le présent Traité doivent être détruites sans délai; le cas échéant, l'État qui a reçu les données prend d'autres mesures conformes à son droit interne qui servent tout aussi bien les droits de la personne concernée.*

3. *Les Parties* contractantes *protègent les données à caractère personnel contre la perte accidentelle, contre la destruction ou la modification accidentelle ou contre l'accès ou l'utilisation non autorisé, contre la divulgation ou contre tout autre abus.*

4. Elles garantissent les droits légitimes de la personne concernée par la transmission des données au titre du présent Traité à l'information et à l'accès aux données la concernant, à leur rectification ou à leur suppression ou, le cas échéant, à la limitation de leur exploitation

---

[101] , RS **0.351.942.7** - Traité d'entraide judiciaire en matière pénale du 4 février 2019 entre la Confédération suisse et la République d'Indonésie (admin.ch) entré en vigueur le 14 septembre 2021.

et, à la demande de la personne concernée, à un recours effectif en lien avec la transmission *ou l'utilisation des informations."*

Lors de clauses contractuelles (art. 16, al. 2, let. a, b et d LPD), il faut tenir compte du fait que celles-ci ne suffisent pas, selon les circonstances, à garantir une protection adéquate[102].

3.3 Délégation législative

Le Conseil fédéral est habilité à adopter des dispositions d'exécution (art. 182 Cst.), c'est-à-dire des normes secondaires qui précisent une disposition légale, décrivent ses effets juridiques, concrétisent des notions juridiques indéterminées ou règlent des questions d'organisation[103]. Dans le domaine de la protection des données, le Conseil fédéral peut, par exemple, préciser les modalités du droit d'accès.

L'art. 164, al. 2 Cst. autorise le législateur à déléguer sa compétence d'édicter des règles de droit primaire, à moins que la Constitution ne l'exclue, par exemple pour les restrictions graves aux droits fondamentaux. Ainsi, la durée de conservation de données sensibles doit respecter le principe de proportionnalité ainsi que le principe de finalité (cf. ci-dessus ch. 2.4) et être prévue dans la loi au sens formel. Elle peut cependant faire l'objet d'une norme de délégation de compétences législatives et la loi au sens formel peut charger le Conseil fédéral de régler la durée de conservation des données traitées (cf. par exemple, l'art. 38, al. 1, let. b *in fine* de la loi sur les prestations de sécurité privées fournies à l'étranger[104]*).*

La norme de délégation doit décrire l'objet, le but (à moins qu'il ne soit évident), l'étendue, et, autant que possible, les grandes lignes de la réglementation déléguées[105].

IV Check-list

Les questions abordées ci-dessus, à se poser lors de l'élaboration de bases légales pour permettre le traitement de données personnelles par des organes fédéraux, sont résumées dans la check-list qui suit:

Questions	**Eléments de réponse**	**Renvois**
Traite-t-on des données personnelles sur une/des personnes physiques ?	Si oui : La LPD s'applique.	Cf. ch. 2.2 et ch. 2.3.1 ci-dessus. Voir aussi Note OFJ relative à la révision totale de la LPD, ch. 4.5.

[102] Voir à ce sujet les explications du PFPDT, Actualités (admin.ch) https://www.edoeb.admin.ch/edoeb/de/home/datenschutz/handel-und-wirtschaft/uebermittlung-ins-ausland.html., .

[103] Guide de législation, n° 721.

[104] RS **935.41** - Loi fédérale du 27 septembre 2013 sur les prestations de sécurité privées fournies à l'étranger (LPSP) (admin.ch)

[105] Guide de législation, n° 721 précité.

Y a-t-il des démarches à accomplir avant de commencer d'élaborer des bases légales ?	Oui. Avant même de commencer d'élaborer les bases légales sur le traitement de données, examine s'il y a lieu de procéder à analyse d'impact en matière de protection des données (AIPD, art. 22 LPD) et élabore un concept SIPD (Sûreté de l'information et protection des données selon la méthode Hermès). Il examine à cet égard l'opportunité de mettre en place des mesures techniques et organisationnelles (protection des données dès la conception et par défaut, cf. art. 7, al. 2 LPD), et les détermine cas échéant. Il consulte les outils spécifiques sur la conduite de projets en matière de digitalisation et les outils généraux en matière de législation.	Cf. introduction ci-dessus. Voir aussi Note OFJ relative à la révision totale de la LPD, ch. 4.3. et 4.5.
La base légale envisagée permette-t-elle la reconnaissabilité du traitement de données pour la personne concernée ?	La base légale qui prévoit un traitement de données personnelles par les organes fédéraux doit préciser qui traite quelles données, dans quel but, (qui, quoi, pourquoi), et, dans certains cas, quel est le mode de traitement.	Cf. ch. 2.4 et ch. 3.1 ci-dessus.
Le traitement de données présente-t-il un risque élevé d'atteinte aux droits fondamentaux de la personne concernée ?	Oui. Conséquences sur le niveau normatif (base légale formelle, au sens de l'art. 34, al. 2, let. c LPD) et sur la densité normative. .	Cf. ch. 1.1, ch. 3.1 et 3.2 ci-dessus. Voir aussi Note OFJ relative à la révision totale de la LPD, ch. 4.3.
Effectue-t-on un traitement de données sensibles au sens du catalogue élargi de l' art. 5, let. c LPD ?	Oui. Conséquences sur la base légale, en principe formelle (art. 34, al. 2, let. a LPD). Pour garantir la transparence du traitement envers la personne	Cf. ch. 2.3.2 et ch. 3.2.1 ci-dessus. Voir aussi Note OFJ relative à la révision totale de la LPD, ch. 2.2.1, let. a.

	concernée, prévoir les catégories visées à l'art. 5, let. c, ch. 1-6 LPD ou des sous-catégories de données sensibles dans les dispositions légales.	
Effectue-t-on des profilages au sens de l'art. 5, let. f LPD ?	Oui. Conséquences sur la base légale, en principe formelle (art. 34, al. 2, let. b LPD). Le but du profilage et les catégories de données sensibles qui sont utilisées pour ce profilage ainsi que les aspects personnels évalués grâce au profilage doivent au minimum être prévus dans la disposition légale.	Cf. ch. 2.3.3 et ch. 3.2.2 ci-dessus. Voir aussi Note OFJ relative à la révision totale de la LPD, ch. 2.2.1, let. b.
La finalité ou le mode de traitement risque-t-il de porter gravement atteinte aux droits fondamentaux ?	Oui. Conséquences possibles sur le niveau normatif (base légale formelle, au sens de l'art. 34, al. 2, let. c LPD) et sur la densité normative.	Cf. ch. 3.2.3 ci-dessus. Voir aussi Note OFJ relative à la révision totale de la LPD, ch. 2.2.1, let cc.
Y a-t-il une décision individuelle automatisée au sens de l'art. 21 LPD ?	Oui. Conséquences possibles sur le niveau normatif (base légale, le plus souvent formelle, au sens de l'art. 34, al. 2, let. c LPD). La logique sur laquelle la décision automatisée repose doit être reconnaissable dans les grandes lignes pour la personne concernée.	Cf. ch. 2.3.4 et ch. 3.2.3 ci-dessus. Voir aussi Note OFJ relative à la révision totale de la LPD, ch. 2.2.1, let. cc.
Y a-t-il un soutien automatisé à la prise de décision (préparation de la décision grâce à un processus automatisé ou voire de l'utilisation d'intelligence artificielle) ?	Oui. Conséquences possibles sur le niveau normatif (base légale, le plus souvent formelle, au sens de l'art. 34, al. 2, let. c LPD).	Cf. ch. 2.3.5 et ch. 3.2.3 ci-dessus. Voir aussi Note OFJ relative à la révision totale de la LPD, ch. 2.2.1, let. cc.
Le responsable du traitement au sens de l'art. 5, let. j LPD est-il identifié ?	Oui. Il doit apparaître comme tel dans les dispositions légales, à l'instar de l'actuel	Cf. ch. 2.3.7 ci-dessus.

	maître du fichier. C'est auprès de lui que s'exerce le droit d'accès. Le responsable du traitement doit de plus garantir que les prescriptions en matière de protection des données sont respectées.	Voir aussi Note OFJ relative à la révision totale de la LPD, ch. 4.1, ch. 4.4.2 et ch. 4.5.
Un organe fédéral traite-t-il des données conjointement avec d'autres organes fédéraux ou cantonaux ou avec des personnes privées au sens de l'art. 33 LPD ?	Oui. Le Conseil fédéral est alors chargé de régler les responsabilités et les procédures de contrôle.	Cf. ch. 2.3.7 ci-dessus. Voir aussi Note OFJ relative à la révision totale de la LPD, ch. 4.1.
Est-il prévu de sous-traiter le traitement des données ?	Oui. Conséquences possibles sur la législation, sinon prévoir la sous-traitance contractuellement.	Cf. ch. 2.3.8 ci-dessus. Voir aussi Note OFJ relative à la révision totale de la LPD, ch. 4.1.
La finalité du traitement est-elle explicite ?	Oui. Elle doit apparaître de manière reconnaissable dans la base légale.	Cf. ch. 2.4 ci-dessus. Voir aussi Note OFJ relative à la révision totale de la LPD, ch. 2.1.
Les autres principes de protection des données, en particulier, la proportionnalité du traitement et l'exactitude des données, seront-ils respectés ?	Oui. S'assurer que les principes de protection des données garantis par le droit international et les limites constitutionnelles aux restrictions aux droits fondamentaux sont respectés (art. 36 Cst.).	Cf. ch. 1.1 ci-dessus. Voir aussi Note OFJ relative à la révision totale de la LPD, ch. 2.1.
Des délais de conservation des données sont-ils prévus ?	Oui, s'assurer que les principes de proportionnalité et de finalité sont respectés.	Cf. ch. 2.4 en relation avec le ch. 3.3
Une communication (y compris un accès aux données personnelles) est-elle prévue ?	Oui. Ils doivent être prévus dans une base légale spécifique qui doit régler : l'autorité responsable de la communication des données ; la finalité de la communication ou de l'accès aux données; les catégories de données concernées;	Cf. ch. 3.2.4 ci-dessus. Voir aussi Note OFJ relative à la révision totale de la LPD, ch. 2.1.

	les modes de communication des données; les destinataires.	
La finalité de la communication (y compris de l'accès aux données) ou le mode de communication risquent-ils de porter gravement atteinte aux droits fondamentaux ?	Oui. Conséquences sur le niveau normatif (base légale formelle, au sens de l'art. 34, al. 2, let. c LPD auquel renvoie l'art. 36, al. 1 LPD) et sur la densité normative.	Cf. ch. 3.2.3 ci-dessus. Voir aussi Note OFJ relative à la révision totale de la LPD, ch. 2.1 et ch. 2.2.2.
Communique-t-on (ou donne-t-on accès) à des données sensibles ?	Oui. Conséquences sur la base légale, en principe formelle (art. 34, al. 2, let. a LPD auquel renvoie l'art. 36, al. 1 LPD).	Cf. ch. 2.3.2 et ch. 3.2.4.1 ci-dessus. Voir aussi Note OFJ relative à la révision totale de la LPD, ch. 2.2.1, let. a.
Communique-t-on (ou donne-t-on accès) à des profilages ?	Oui. Conséquences sur la base légale, en principe formelle (art. 34, al. 2, let. b LPD auquel renvoie l'art. 36, al. 1 LPD).	Cf. ch. 2.3.3 et ch. 3.2.4.1 ci-dessus. Voir aussi Note OFJ relative à la révision totale de la LPD, ch. 2.2.1, let. b.
Communique-t-on (ou donne-t-on accès à) des données à l'étranger ?	Oui. S'assurer que la législation de l'État destinataire assure un niveau de protection adéquat au sens de l'art. 16, al. 1 LPD ou que les conditions posées par l'art. 16, al. 2 LPD sont remplies.	Cf. ch. 3.2.5 ci-dessus. Voir aussi Note OFJ relative à la révision totale de la LPD, ch. 4 et ch. 4.2.
Une délégation législative est-elle prévue ?	Oui. S'assurer qu'elle respecte les principes de la délégation législative.	Cf. ch 3.3 ci-dessus.