

C
E
R
T

Valérie Défago | Jean-Philippe Dunand
Pascal Mahon | Samah Posse | David Raedler (éds)

François Charlet | Frédéric Erard
Célian Hirsch | Sylvain Métille
Samah Posse | David Raedler

La protection des données dans les relations de travail à la lumière de la nouvelle loi fédérale sur la protection des données





Valérie Défago
Jean-Philippe Dunand
Pascal Mahon

Volume 19

Valérie Défago | Jean-Philippe Dunand | Pascal Mahon
Samah Posse | David Raedler (éds)

François Charlet | Frédéric Erard
Célian Hirsch | Sylvain Métille
Samah Posse | David Raedler

La protection des données dans les relations de travail à la lumière de la nouvelle loi fédérale sur la protection des données



Schulthess § 2024
ÉDITIONS ROMANDES

Citation suggérée de l'ouvrage: VALÉRIE DÉFAGO / JEAN-PHILIPPE DUNAND / PASCAL MAHON / SAMAH POSSE / DAVID RAEDLER (éds), *La protection des données dans les relations de travail à la lumière de la nouvelle loi fédérale sur la protection des données*, « Collection CERT », Genève/Zurich 2024, Schulthess Éditions Romandes

ISBN 978-3-7255-8976-0

© Schulthess Médias Juridiques SA, Genève · Zurich 2024
www.schulthess.com

Diffusion en France : Lextenso Éditions, La Grande Arche, Paroi Nord 1 Parvis de La Défense 92044 Paris – La Défense
www.lextenso-editions.com

Diffusion en Belgique et au Luxembourg : Patrimoine, 119, avenue Milcamps, 1030 Bruxelles

Tous droits réservés. Toute traduction, reproduction, représentation ou adaptation intégrale ou partielle de cette publication, par quelque procédé que ce soit (graphique, électronique ou mécanique, y compris photocopie et microfilm), et toutes formes d'enregistrement sont strictement interdites sans l'autorisation expresse et écrite de l'éditeur.

Information bibliographique de la Deutsche Nationalbibliothek : La Deutsche Nationalbibliothek a répertorié cette publication dans la Deutsche Nationalbibliografie ; les données bibliographiques détaillées peuvent être consultées sur Internet à l'adresse <http://dnb.d-nb.de>.

Table des matières

Table des abréviations.....	IX
-----------------------------	----

Première partie : Principes généraux et enjeux

Loi fédérale sur la protection des données révisée : principes généraux et nouveautés.....	3
---	----------

Sylvain Métille

Docteur en droit, avocat, professeur associé à l'Université de Lausanne

Protection des données : enjeux et risques pour les entreprises.....	49
---	-----------

François Charlet

Chief Privacy & Data Protection Officer, co-fondateur de l'Association suisse des délégués à la protection des données

Deuxième partie : Questions spécifiques

La collecte des données relatives à la santé des travailleurs par l'employeur privé.....	65
---	-----------

Frédéric Erard

Professeur associé à l'Université de Lausanne

Droit du travail et intelligence artificielle : défis des décisions automatisées pour les employeurs.....	97
--	-----------

Célian Hirsch

Docteur en droit, avocat, maître-assistant à l'Université de Genève, lecteur à l'Université de Fribourg

La surveillance numérique des employés – Entre risques et opportunités.....	123
--	------------

Samah Posse

Docteure en droit, chargée d'enseignement à l'Université de Neuchâtel, Chargée de cours & Data Protection Officer à UniDistance Suisse

**Les nouvelles procédures de la LPD révisée et leur impact
dans les rapports de travail**153

David Raedler

Docteur en droit, avocat, spécialiste FSA en droit du travail, Lausanne

Loi fédérale sur la protection des données révisée : principes généraux et nouveautés

Sommaire	Page
I. Introduction	4
II. Quelques notions générales	5
A. Les données personnelles	5
B. Les acteurs	7
III. Des atteintes présumées à la personnalité et de possibles justifications	8
A. Les cas d'atteintes à la personnalité	8
B. Les motifs justificatifs pour les responsables du traitement privés	10
1. Le principe	10
2. Le consentement	10
3. L'intérêt privé	11
4. L'intérêt public	13
5. La loi	13
IV. Quels sont ces grands principes ?	13
A. La bonne foi	13
B. La licéité	14
C. La proportionnalité	14
D. La finalité	15
E. La transparence	16
F. L'exactitude	17
G. La sécurité	18
V. Quelles sont les obligations du responsable du traitement ?	19
A. Les obligations déjà connues de l'aLPD	19
1. Le transfert à l'étranger	19
2. La sous-traitance	21
3. Le conseiller à la protection des données	22

* Je remercie sincèrement M. QUENTIN JACQUEMIN pour son aide précieuse dans la mise en forme de cette contribution. Les conférences sur la LPD ont été nombreuses ces derniers mois, comme les publications. Il est difficile d'être original et on ne peut guère inventer d'autres nouveautés ou principes. Certains passages sont donc inspirés de contributions précédentes et mis à jour. Que l'on n'y voie ni une paresse ni un auto-plagiat, mais simplement une cohérence des propos et une transparence assumée par cette note.

B. Les nouvelles obligations	24
1. Le registre des activités de traitement	24
2. L'analyse d'impact relative à la protection des données personnelles	25
3. L'information	27
4. L'annonce des violations de la sécurité des données	30
5. Le représentant	32
6. La protection des données dès la conception et protection des données par défaut	33
VI. Les droits de la personne concernée	34
A. Les droits déjà connus de l'aLPD	34
1. Les droits d'opposition et de correction	34
2. Le droit d'accès	36
B. Les nouveaux droits	38
1. En matière d'information	38
2. En matière de décision individuelle automatisée	38
3. Le droit à la remise ou à la transmission des données	39
VII. La procédure et la surveillance	40
VIII. Conclusion	43
Bibliographie	45

I. Introduction

Le Parlement fédéral a adopté la Loi fédérale (révisée) sur la protection des données (LPD) le 25 septembre 2020¹. Elle est entrée en vigueur le 1^{er} septembre 2023, abrogeant la Loi fédérale sur la protection des données du 19 juin 1992 (aLPD). L'Ordonnance sur la protection des données du 31 août 2022 (OPDo) a simultanément remplacé l'Ordonnance du 14 juin 1993 relative à la loi fédérale sur la protection des données (OLPD).

Même s'il s'agit techniquement d'une révision totale, il faut bien plus y voir une mise à jour de l'aLPD. En effet, la structure et la logique de la loi demeurent inchangées. Les grands principes (IV) sont conservés, de même que les notions générales (II) sous réserve de la notion de personne concernée qui se limite désormais aux personnes physiques.

On trouve des nouveautés principalement au niveau des obligations du responsable du traitement et du sous-traitant (V), des droits des personnes concernées (VI), de la procédure et des sanctions pénales (VII).

¹ Sur le long processus qui a pris plus de 10 ans, voir notamment : MÉTILLE, Traitement de données, pp. 1 ss.

Conformément à la demande des éditeurs scientifiques, une première partie sera consacrée aux notions et principes généraux et la seconde aux principales nouveautés. Par souci de concision, le propos est limité au droit suisse² et aux responsables du traitement privés³.

II. Quelques notions générales

A. Les données personnelles

La notion de données personnelles est large et inclut toutes les informations concernant une personne physique identifiée ou identifiable (art. 5 let. a LPD)⁴. Une personne est identifiée lorsque l'on sait de qui il s'agit. Elle est identifiable lorsqu'elle peut être identifiée, directement ou indirectement, sur la base d'un ou plusieurs éléments. Un nom, une adresse électronique, un numéro de téléphone, une adresse IP, un numéro AVS, une empreinte digitale, une adresse ou une date de naissance sont des données personnelles.

Les données pseudonymes sont des données personnelles puisque la personne demeure identifiable⁵. Si ce n'est pas le cas, on parlera de données anonymes⁶. Les données anonymes ne sont pas soumises à la LPD. Une possibilité purement théorique qu'une personne soit identifiée n'est pas suffisante. La possibilité d'identifier la personne concernée doit s'apprécier de façon relative, soit selon le point de vue de l'intéressé⁷. Des données pseudonymes constituent des données personnelles seulement du point de vue de celui qui détient la table de concordance⁸ ou de celui qui pourrait réidentifier la personne

² Pour des considérations liées au RGPD, on peut notamment renvoyer à : MÉTILLE/ARASTEH, pp. 107 ss ; MÉTILLE/ACKERMANN, pp. 77 ss ; MÉTILLE, Nouvelle loi, pp. 1 ss, et les nombreuses références citées.

³ Nombre de considérations s'appliquent néanmoins également aux organes fédéraux. Les principales différences concernent l'exigence de la base légale (art. 34 LPD) et l'absence de recours aux motifs justificatifs de l'art. 31 LPD, ainsi que les prétentions et la procédure régie par l'art. 41 LPD et la Loi fédérale sur la procédure administrative du 20 décembre 1968 (PA ; RS 172.021), plutôt que le Code de procédure civile du 19 décembre 2008 (CPC ; RS 272). Sur le traitement par les organes fédéraux, voir notamment : BELSER/EPINEY/WALDMANN et EPINEY/NÜESCH/ROVELLI.

⁴ Sur la notion de données personnelles, voir notamment : ROSENTHAL, nDSG, N 19 ss ; CR LPD-MEIER/TSCHUMY, art. 5 N 18 ss ; SHK DSG-RUDIN, art. 5 N 2 ss.

⁵ CR LPD-MEIER/TSCHUMY, art. 5 N 29.

⁶ Sur la notion de données anonymes, de données pseudonymes et le risque de réidentification, voir les nombreuses contributions réunies dans : MÉTILLE, Protection des données et recherche.

⁷ CR LPD-MEIER/TSCHUMY, art. 5 N 25 et 27.

⁸ TF 4A_365/2017 du 26 février 2018, c. 5.1.1.

en mettant en œuvre des moyens raisonnables⁹. Ne seraient pas raisonnables des moyens interdits par la loi ou irréalisables en pratique (ou au prix d'efforts démesurés en termes de temps, de coût et de main-d'œuvre).

L'art. 5 let. c LPD prévoit que certaines données personnelles sont sensibles¹⁰. C'est le cas des données sur les opinions ou les activités religieuses, philosophiques, politiques ou syndicales (art. 5 let. c ch. 1 LPD) ; des données sur la santé¹¹, la sphère intime ou l'origine raciale ou ethnique (art. 5 let. ch. 2 LPD) ; des données génétiques (art. 5 let. c ch. 3 LPD) ; des données biométriques identifiant une personne physique de manière univoque (art. 5 let. c ch. 4 LPD)¹² ; des données sur des poursuites ou sanctions pénales et administratives (art. 5 let. c ch. 5 LPD) ; ainsi que des données sur des mesures d'aide sociale (art. 5 let. c ch. 6 LPD).

Contrairement à ce que prévoit le RGPD¹³, le traitement de données sensibles n'est pas interdit par principe, mais il demande une plus grande prudence et peut déclencher quelques obligations supplémentaires comme une analyse d'impact préalable en cas de traitement à grande échelle (art. 22 al. 2 let. a LPD) ou un consentement pour pouvoir les traiter dans le but d'évaluer la solvabilité¹⁴. Si un consentement est requis, il doit être exprès (art. 6 al. 7 LPD). Contrairement à une croyance trop répandue, ce n'est pas parce que des données sensibles sont traitées qu'un consentement est nécessaire. L'art. 6 al. 7 LPD ne porte que sur la nature du consentement et n'introduit pas une exigence de consentement pour tout traitement de données sensibles¹⁵.

La LPD a introduit les notions de profilage (art. 5 let. f LPD) et de profilage à risque élevé (art. 5 let. g LPD)¹⁶. Le profilage recouvre toute forme de traitement automatisé de données personnelles consistant à utiliser ces données pour évaluer certains aspects personnels relatifs à une personne physique, notamment pour analyser ou prédire des éléments concernant le rendement au travail, la situation économique, la santé, les préférences personnelles, les intérêts, la fiabilité, le comportement, la localisation ou les déplacements

⁹ Message nLPD, FF 2017 6639 ss ; CJUE, aff. C-582/ 14, ECLI:EU:C:2016:779, c. 42 ss.

¹⁰ Sur cette notion, voir notamment : CR LPD-MEIER/TSCHUMY, art. 5 N 43 ss ; SHK DSG-RUDIN, art. 5 N 19 ss.

¹¹ Sur les données liées à la santé, voir FRÉDÉRIC ERARD, pp. 65 ss du présent ouvrage.

¹² Les données génétiques et les données biométriques ne figuraient pas dans l'aLPD.

¹³ Art. 9 RGPD.

¹⁴ Art. 31 al. 2 let. c LPD.

¹⁵ CR LPD-MEIER/TSCHUMY, art. 6 N 93 ; ROSENTHAL, nDSG, N 32 ; SHK DSG-BAERISWYL, art. 6 N 104.

¹⁶ La notion de profilage à risque élevé a été introduite par le Conseil des Etats (CR LPD-MEIER/TSCHUMY, art. 5 N 94). Ce n'est qu'en ultime séance de conciliation que les chambres fédérales ont réussi à se mettre d'accord sur cette notion.

de cette personne physique. Pour certains auteurs, le profilage débute là où s'arrêterait le profil de personnalité : il faut un traitement automatisé et un but d'évaluation¹⁷. Pour d'autres, tout profilage donnant lieu à l'établissement d'un profil de la personnalité devrait être considéré comme un profilage à risque élevé¹⁸. La notion de traitement automatisé n'exige pas de recours à l'intelligence artificielle ou d'algorithme, car il suffit que le traitement ne soit pas manuel¹⁹.

Quant au profilage à risque élevé, c'est celui qui entraîne un risque élevé pour la personnalité ou les droits fondamentaux de la personne concernée, parce qu'il conduit à un appariement de données qui permet d'apprécier les caractéristiques essentielles de la personnalité d'une personne physique (art. 5 let. g LPD).

La différence entre profilage et profilage à risque élevé a beaucoup occupé l'Assemblée fédérale, mais ses conséquences concrètes sont limitées²⁰. En pratique et pour les traitements privés, c'est seulement le profilage à risque élevé qui a des conséquences légales²¹. Par exemple, si un consentement est requis, le consentement doit être exprès lorsqu'il s'agit d'un profilage à risque élevé (art. 6 al. 7 let. b LPD). Finalement, le profilage à risque élevé n'est pas permis dans le but d'évaluer la solvabilité de la personne concernée, ou plus justement dit, le responsable du traitement privé ne peut pas faire valoir un intérêt prépondérant à effectuer un profilage à risque élevé dans ce but²².

B. Les acteurs

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

La personne concernée est la personne physique, identifiée ou identifiable, dont les données personnelles font l'objet d'un traitement (art. 5 let. b LPD). C'est sa personnalité que la LPD veut protéger (art. 1 LPD). Contrairement à l'aLPD, les données de personnes morales ne sont plus protégées par la LPD²³. La Suisse s'aligne ainsi sur les autres pays, ce qui devrait faciliter grandement le transfert de données à l'étranger²⁴. Les personnes

¹⁷ ROSENTHAL, nDSG, N 24.

¹⁸ JACOT-GUILLARMOD.

¹⁹ CR LPD-MEIER/TSCHUMY, art. 5 N 92 et les références citées.

²⁰ ROSENTHAL, nDSG, N 28.

²¹ Pour les organes fédéraux, voir : CR LPD-MEIER/TSCHUMY, art. 5 N 93.

²² Une autre justification est en revanche envisageable, en particulier le consentement de la personne concernée.

²³ CR LPD-MEIER/TSCHUMY, art. 5 N 31 ; SHK DSG-RUDIN, art. 5 N 18.

²⁴ En particulier vers les pays offrant un niveau de protection adéquat pour les personnes physiques.

morales peuvent continuer à invoquer la protection générale de leur personnalité garantie par les art. 28 ss du CC²⁵.

Le responsable du traitement²⁶ 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 (art. 5 let. j LPD). Les modalités du traitement concernent les aspects formels (processus de traitement, logiciels utilisés, mesures de sécurité), et les paramètres matériels du traitement (le type de données traitées, leurs sources, les opérations de traitement, etc.)²⁷.

Le sous-traitant est la personne privée ou l'organe fédéral qui traite des données personnelles pour le compte et selon les instructions du responsable du traitement (art. 5 let. k LPD). Cette notion n'était pas définie dans l'aLPD²⁸.

Le destinataire est la personne privée ou l'organe fédéral à qui des données sont transférées. Il peut intervenir en qualité de tiers (responsable du traitement indépendant) ou de sous-traitant²⁹.

III. Des atteintes présumées à la personnalité et de possibles justifications

A. Les cas d'atteintes à la personnalité

La notion de traitement est très large et recouvre toute opération relative à des données personnelles, indépendamment des moyens et procédés utilisés (art. 5 let. d LPD). Cela inclut par exemple la collecte, l'enregistrement, la conservation, l'utilisation, la modification, la communication, l'archivage, l'effacement ou la destruction de données³⁰.

²⁵ Cette modification a néanmoins eu un impact légistique pour les organes fédéraux. En effet, les bases légales qui permettent le traitement de données personnelles ne permettent plus que le traitement de données de personnes physiques, alors que les personnes morales bénéficient de la protection de la sphère privée garantie par la Constitution fédérale du 18 avril 1999 (Cst. ; RS 101) et une base légale reste nécessaire conformément à son art. 36. De nombreuses lois ont donc dû être complétées (Message nLPD, FF 2017 6595 et Message nLPD, FF 2017 6632).

²⁶ Le maître du fichier dans la terminologie de l'aLPD, ainsi que dans certains cantons (CR LPD-MEIER/TSCHUMY, art. 5 N 107).

²⁷ ROSENTHAL, Controller oder Processor, N 33.

²⁸ CR LPD-MEIER/TSCHUMY, art. 5 N 112.

²⁹ MEIER, Précis, N 612 ss.

³⁰ BSK DSG-BLECHTA, art. 3 N 71 ss ; CR LPD-MEIER/TSCHUMY, art. 5 N 72.

Dans sa concrétisation de la protection générale de la personnalité, la LPD prévoit des situations dans lesquelles le traitement est considéré comme constituant une atteinte à la personnalité. L'art. 30 al. 2 LPD prévoit trois cas de figure différents : lorsque des données personnelles sont traitées en violation des principes (let. a), lorsque des données personnelles sont traitées contre la manifestation expresse de la volonté de la personne concernée (let. b), ou lorsque des données personnelles sensibles sont communiquées à des tiers (let. c). C'est une présomption irréfragable et la personne concernée n'a pas besoin de démontrer une atteinte à sa personnalité³¹. Elle doit, le cas échéant, seulement prouver qu'elle est dans un des cas de figure précités.

L'énumération de l'art. 30 al. 2 LPD n'est pas exhaustive et une autre situation peut constituer une atteinte à la personnalité³². La personne concernée ne bénéficie alors pas de la présomption légale et devra démontrer *in casu* l'existence de l'atteinte.

Ce principe est atténué par l'art. 30 al. 3 LPD qui précise qu'il n'y a en règle générale pas d'atteinte lorsque la personne concernée a rendu les données personnelles accessibles à tout un chacun et ne s'est pas opposée expressément au traitement. C'est une présomption légale réfragable de non-atteinte³³. Le responsable du traitement doit démontrer que les données ont été rendues accessibles à tout un chacun par la personne concernée (consciemment et volontairement), alors que la personne concernée doit démontrer qu'elle s'est opposée formellement au traitement et que cette opposition a bien été reçue³⁴.

Le premier cas de traitement illicite prévu par la loi concerne la violation des principes figurant aux art. 6 et 8 LPD³⁵ et qui doivent guider tout traitement de données³⁶.

Le deuxième cas de traitement illicite est celui où la personne concernée s'oppose. Ce droit inconditionnel de s'opposer à certains traitements est la concrétisation au plan privé du droit à l'autodétermination informationnelle figurant à l'art. 13 al. 2 Cst.³⁷. L'opposition n'est pas soumise à une exigence de forme et n'a pas besoin de justification, mais elle doit être expresse³⁸. C'est une simple déclaration de volonté soumise à réception qui doit porter sur des auteurs de traitement déterminés ou déterminables³⁹. Elle peut porter seulement sur

³¹ CR LPD-BOILLAT/WERLY, art. 30 N 16.

³² Message nLPD, FF 2017 6688.

³³ Message nLPD, FF 2017 6688 ; CR LPD-BOILLAT/WERLY, art. 30 N 36.

³⁴ MEIER, Précis, N 1592 ss.

³⁵ La protection des données dès la conception et la protection des données par défaut (art. 7 LPD) ne sont pas des principes à proprement parler, mais bien plus des obligations à charge du responsable du traitement. Leur violation ne rend pas le traitement illicite au sens de l'art. 30 LPD.

³⁶ CR LPD-BOILLAT/WERLY, art. 30 N 17 ; SHK DSG-PFAFFINGER, art. 30 N 31.

³⁷ MEIER, Précis, N 1553 ; CR LPD-BOILLAT/WERLY, art. 30 N 26 ss ; PC LPD-GENECAND, art. 30 N 8.

³⁸ MEIER, Précis, N 1559 ; Message nLPD, FF 2017 6688.

³⁹ MEIER, Précis, N 1558 ; Message nLPD, FF 2017 6688.

certaines finalités. Une manifestation de volonté « tacite » comme le fait de ne plus utiliser activement un service n'est pas suffisante⁴⁰.

Le troisième cas concerne une situation jugée particulièrement risquée, car il y a le cumul de données sensibles et le transfert à des tiers. Ce double risque justifie de considérer ce traitement comme une atteinte illicite⁴¹.

B. Les motifs justificatifs pour les responsables du traitement privés

1. Le principe

Une atteinte à la personnalité est présumée illicite⁴². Cette présomption, contrairement à celle de l'atteinte que nous avons vue ci-dessus, est réfragable. Cela signifie que si le responsable du traitement ne peut pas remettre en cause l'atteinte à la personnalité, il peut y opposer des motifs justificatifs qui rendront l'atteinte licite⁴³.

Pour assurer une certaine sécurité du droit, la LPD énumère les motifs justificatifs. Une atteinte à la personnalité est considérée comme licite si elle peut être justifiée par le consentement de la personne concernée, un intérêt prépondérant privé, un intérêt prépondérant public, ou par la loi (art. 31 al. 1 LPD).

2. Le consentement

Le premier motif justificatif est le consentement de la personne concernée. Pour qu'il soit valable, la personne concernée doit avoir exprimé librement et clairement sa volonté concernant un ou plusieurs traitements déterminés et après avoir été dûment informée (art. 6 al. 6 LPD). Il doit être exprès dans les cas d'un traitement de données sensibles ou d'un profilage à risque élevé (art. 6 al. 7 LPD)⁴⁴.

⁴⁰ Message nLPD, FF 2017 6688.

⁴¹ MEIER, Précis, N 1556.

⁴² CR LPD-BOILLAT/WERLY, art. 30 N 1 ; SHK DSG-PFAFFINGER, Vorbem. zu Art. 30-32 N 24.

⁴³ CR LPD-BOILLAT/WERLY, art. 31 N 19 ss ; PC LPD-GENECAND, art. 30 N 3.

⁴⁴ Lorsque le consentement est requis, il doit être exprès seulement pour un profilage à risque élevé effectué par une personne privée. Si le profilage est l'œuvre d'un organe fédéral, le consentement (s'il est requis) doit être exprès qu'il s'agisse d'un profilage simple ou à risque élevé.

La notion de consentement libre et éclairé vient de la jurisprudence applicable en droit médical⁴⁵. Un consentement est libre si la personne n'a pas subi de menace, de pression déraisonnable, directe ou indirecte (de la part du responsable du traitement ou d'un tiers).

Subir un désavantage en l'absence de consentement ne signifie pas forcément que le consentement n'est pas libre, mais le consentement ne sera pas libre si le désavantage est sans rapport avec le but du traitement ou manifestement disproportionné⁴⁶. Il n'est pas obligatoire de fournir une alternative pour que le consentement puisse être libre⁴⁷, mais s'il y a une alternative, c'est un fort indice de liberté de consentir. La liberté du consentement présuppose aussi que les informations qui ne sont pas obligatoires soient présentées comme telles⁴⁸.

Le consentement est éclairé si la personne concernée a reçu une information objective, complète et compréhensible sur le traitement envisagé, en particulier sur le responsable du traitement, les finalités, le type et l'étendue des données traitées, les opérations de traitement envisagées, etc.⁴⁹. La personne doit donc disposer de tous les éléments qui au vu des circonstances, lui permettent de prendre une décision en toute connaissance de cause.

Le consentement devrait être donné par un acte positif clair par lequel la personne concernée manifeste de façon libre, spécifique, éclairée et univoque son accord au traitement. L'expression du consentement peut se faire par oral ou par écrit, y compris en cochant une case lors de la consultation d'un site web. Il n'y a en revanche pas de consentement en cas de silence, de cases cochées par défaut ou d'inactivité⁵⁰.

3. L'intérêt privé

Le deuxième motif justificatif est l'intérêt privé prépondérant. L'art. 31 al. 2 LPD dresse une liste non exhaustive d'intérêts qui sont en principe reconnus comme prépondérants. C'est le plus souvent l'intérêt du responsable du traitement, mais parfois aussi celui de la personne concernée voire d'un tiers⁵¹.

⁴⁵ MEIER, Précis, N 831.

⁴⁶ CR LPD-BOILLAT/WERLY, art. 31 N 21.

⁴⁷ MEIER, Précis, N 859.

⁴⁸ MEIER, Précis, N 705 et 852 ss.

⁴⁹ MEIER, Précis, N 861.

⁵⁰ CR LPD-BOILLAT/WERLY, art. 31 N 21.

⁵¹ PC LPD-GENECAND, art. 31 N 25.

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

Il n'y a guère de changement dans la LPD parmi les principaux intérêts prépondérants du responsable du traitement⁵². Ainsi, la liste correspond pour l'essentiel à celle de l'aLPD. On retrouve donc l'hypothèse où le traitement est en relation directe avec la conclusion ou l'exécution d'un contrat, pour autant que les données traitées concernent le cocontractant (art. 31 al. 2 let. a LPD). On retrouve également le cas selon lequel le traitement s'inscrit dans un rapport de concurrence actuel ou futur avec une autre personne, pour autant que les données ne soient pas communiquées à des tiers (art. 31 al. 2 let. b LPD). S'agissant des données personnelles traitées de manière professionnelle exclusivement en vue d'une publication dans la partie rédactionnelle d'un média à caractère périodique, ou qui servent exclusivement d'instrument de travail personnel si la publication n'a pas lieu, ce cas est prévu à l'art. 31 al. 2 let. d LPD. Finalement, le cas des données personnelles recueillies concernant une personnalité publique et se référant à son activité publique est prévu à l'art. 31 al. 2 let. f LPD.

A certaines conditions, les données personnelles traitées dans le but d'évaluer la solvabilité de la personne concernée représentent aussi un intérêt prépondérant (art. 31 al. 2 let. c LPD)⁵³. Après de nombreuses discussions, l'Assemblée fédérale a finalement décidé que ces données, qui ne doivent représenter ni des données sensibles ni un profilage à risque élevé, ne doivent pas dater de plus de dix ans et ne pas concerner des personnes mineures⁵⁴. Les données ne peuvent être communiquées à des tiers que s'ils en ont besoin pour conclure ou exécuter un contrat avec la personne concernée.

Finalement, il y a un large intérêt dans le cadre de la recherche, de la planification ou de la statistique⁵⁵. Des données personnelles peuvent y être traitées pour autant qu'elles le soient à des fins ne se rapportant pas à des personnes. Le responsable du traitement doit en outre les anonymiser dès que possible⁵⁶, ne pas communiquer à des tiers des données sensibles sous une forme permettant d'identifier la personne concernée et ne pas publier de résultats sous une forme permettant d'identifier les personnes concernées.

⁵² CR LPD-BOILLAT/WERLY, art. 31 N 3 et 30.

⁵³ ROSENTHAL, nDSG, N 42 ; Message nLPD, FF 2017 6690 ss.

⁵⁴ CR LPD-BOILLAT/WERLY, art. 31 N 49 ss.

⁵⁵ L'art. 39 LPD prévoit que les organes fédéraux peuvent également traiter des données à des conditions similaires sans devoir respecter les principes de finalité et de base légale.

⁵⁶ Cette condition est déjà réalisée lorsque les données sont communiquées sous une forme pseudonymisée et que la clé pour réidentifier la personne reste chez celui qui transmet les données (Message nLPD, FF 2017 6692).

4. L'intérêt public

Le troisième motif, l'intérêt public prépondérant, est assez rare dans le cas de traitements de données personnelles effectués par un privé. Il n'est pas défini par la LPD, mais on peut retenir qu'il y a un intérêt public lorsque l'atteinte est destinée à procurer un avantage à la collectivité ou au moins à une pluralité de personnes⁵⁷.

L'intérêt public prépondérant peut aussi intervenir en soutien d'un intérêt privé. C'est par exemple le cas de l'intérêt d'une assurance privée à ne pas servir des prestations indues ainsi que celui de la collectivité des assurés à ne pas voir les coûts de leurs assurances augmenter⁵⁸. On parle parfois aussi d'intérêt quasi public pour les intérêts cumulés de nombreuses personnes.

5. La loi

Le quatrième motif justificatif est une disposition légale de droit fédéral ou cantonal, qui impose le traitement, le permet ou le suppose en lien avec d'autres obligations qu'elle prévoit. Lorsque la loi sert de motif justificatif, cela signifie que le législateur a déjà procédé à une pesée d'intérêts. C'est par exemple le cas de l'examen de la capacité de contracter un crédit (art. 23 ss LCC), de l'obligation de conserver les pièces comptables (art. 957 et 962 CO), ainsi que de l'Olico⁵⁹ et de l'enregistrement de conversations téléphoniques lors de commandes (art. 179^{quinquies} CP)⁶⁰.

IV. Quels sont ces grands principes ?

A. La bonne foi

Tout traitement de données personnelles doit être effectué conformément au principe de la bonne foi (art. 6 al. 2 LPD). Si le principe de la bonne foi est un principe général de l'ordre juridique suisse (art. 2 CC), celui-ci se traduit, dans le domaine de la protection des données, par le fait qu'aucune donnée ne doit être traitée à l'insu de la personne concernée ou contre sa volonté⁶¹. Celui qui, lors de la collecte des données, laisse croire à la personne

⁵⁷ CR LPD-BOILLAT/WERLY, art. 31 N 26 ; SHK DSG-PFAFFINGER, art. 31 N 45.

⁵⁸ ATF 135 I 169, JdT 2010 I 191 ; ATF 136 III 410, c. 2.2.3, JdT 2010 I 553.

⁵⁹ SHK DSG-PFAFFINGER, art. 31 N 14.

⁶⁰ CR LPD-BOILLAT/WERLY, art. 31 N 22.

⁶¹ CR LPD-MEIER/TSCHUMY, art. 6 N 25 ; PC LPD-FRANCEY, art. 6 N 18.

concernée que toutes les données sont obligatoires alors que certaines sont facultatives, viole le principe de la bonne foi⁶².

B. La licéité

L'art. 6 al. 1 LPD prévoit que tout traitement de données personnelles doit être licite. La notion de licéité doit se comprendre ici comme l'absence de violation d'une norme impérative du droit de la protection des données ou d'une norme visant à protéger la personnalité⁶³, par exemple obtenir ou traiter des données en violation d'un secret⁶⁴. Dans le cadre d'un arrêt opposant le PFPDT à la société suisse d'assurances Helsana, le Tribunal administratif fédéral a précisé que le principe de licéité était violé seulement lorsqu'une norme légale visant la protection de la personnalité était violée, et pas n'importe quelle norme légale⁶⁵.

Pour les organes fédéraux, il est important de rappeler que le principe de licéité impose l'exigence de la base légale : des données personnelles ne peuvent être traitées que s'il existe une base légale (art. 34 al. 1 LPD). Elle doit même être formelle s'il s'agit de données sensibles, d'un profilage ou qu'il y a un risque de porter gravement atteinte aux droits fondamentaux de la personne concernée (art. 34 al. 2 LPD)⁶⁶. Une base légale matérielle peut néanmoins suffire si le traitement est indispensable à l'accomplissement d'une tâche définie dans une loi formelle et que la finalité du traitement ne présente pas de risques particuliers (art. 34 al. 3 LPD)⁶⁷.

C. La proportionnalité

Tout traitement de données personnelles doit être effectué conformément au principe de proportionnalité (art. 6 al. 2 LPD). Ce principe se divise en trois sous-principes de nécessité, aptitude ou adéquation et proportionnalité au sens étroit⁶⁸. Ainsi, le responsable

⁶² MÉTILLE, *Traitement de données*, p. 8.

⁶³ CR LPD-MEIER/TSCHUMY, art. 6 N 19 ; BSK DSG-MAURER-LAMBROU/STEINER, art. 4 N 5 ss.

⁶⁴ Art. 320 ss CP et 47 de la Loi fédérale sur les banques et les caisses d'épargne (Loi sur les banques) du 8 novembre 1934 (LB ; RS 952.0).

⁶⁵ TAF A-3548/2018 du 19 mars 2019, c. 5.4.4. Dans le cadre de cette affaire, le Tribunal administratif fédéral est arrivé à la conclusion que les art. 61 ss de la Loi fédérale sur l'assurance-maladie du 18 mars 1994 (LAMal ; RS 832.10) ne visent pas à protéger la personnalité des personnes assurées, ce faisant leur possible violation est sans effet sur la protection des données.

⁶⁶ CR LPD-MEIER/TSCHUMY, art. 6 N 22 ; SHK DSG-MUND, art. 34 N 11 ss.

⁶⁷ Sur ce point, voir notamment : CR LPD-EPINEY/POSSE, art. 34 N 57 ss.

⁶⁸ CR LPD-MEIER/TSCHUMY, art. 6 N 27.

du traitement ne peut traiter que les données qui sont objectivement nécessaires pour atteindre le but poursuivi, qui sont aptes à l'atteindre, et pour autant que le traitement demeure dans un rapport raisonnable entre le résultat légitime recherché et le moyen utilisé, tout en préservant le plus possible le droit des personnes concernées.

En protection des données, on déduit aussi du principe de proportionnalité les principes d'évitement et de minimisation (ou d'économicité) des données. Le premier implique que si le but du traitement peut être atteint sans collecte de données nouvelles, cette option doit être privilégiée⁶⁹. Le second veut que seules les données absolument nécessaires au but poursuivi soient traitées⁷⁰.

Le principe de proportionnalité s'applique aux types et aux catégories de données traitées, aux moyens de traitement, aux finalités, à la durée de conservation, etc.⁷¹. Compte tenu des évolutions technologiques et des capacités presque illimitées de stockage, le Conseil fédéral a estimé qu'il était important de mentionner expressément que les données doivent être détruites ou anonymisées dès qu'elles ne sont plus nécessaires au regard des finalités du traitement (art. 6 al. 4 LPD)⁷², même si cela découle déjà du principe de proportionnalité, dans son aspect temporel. Pour le Conseil fédéral, il résulte de ce principe que le responsable du traitement doit fixer des délais de conservation⁷³.

D. La finalité

L'art. 6 al. 3 LPD consacre le principe de finalité ou de respect du but : des données personnelles ne peuvent être collectées que pour des finalités déterminées et reconnaissables pour la personne concernée. Le caractère déterminé des finalités implique que des buts vagues, non définis ou imprécis ne suffisent pas⁷⁴. Cela s'apprécie évidemment selon les circonstances, l'objectif étant principalement de concilier les intérêts des personnes concernées et ceux du responsable du traitement. En cas de communication des données à un tiers, ce dernier est lié par les finalités indiquées au moment de la collecte⁷⁵.

⁶⁹ MEIER, Précis, N 671 ss ; PC LPD-FRANCEY, art. 6 N 25 ; Message nLPD, FF 2017 6644.

⁷⁰ CR LPD-MEIER/TSCHUMY, art. 6 N 33 ; PC LPD-FRANCEY, art. 6 N 25.

⁷¹ MEIER, Précis, N 676.

⁷² Message nLPD, FF 2017 6645.

⁷³ *Ibidem*.

⁷⁴ CR LPD-MEIER/TSCHUMY, art. 6 N 50 ; Message nLPD, FF 2017 6644.

⁷⁵ MEIER, Précis, N 726 ; SHK DSG-BAERISWYL, art. 6 N 47.

La LPD précise désormais que les données peuvent également être traitées ultérieurement de manière compatible avec les finalités initiales⁷⁶. Le traitement de données liées à l'octroi d'un prêt par une banque pour vérifier spontanément si le client est éligible à un meilleur type de prêt est une finalité compatible avec la finalité initiale, contrairement à la communication des données à un tiers qui souhaite proposer une assurance responsabilité civile au client de la banque.

Cette nouvelle formulation de la LPD n'implique toutefois pas de changement majeur puisqu'un traitement ultérieur, que la personne concernée considérerait légitimement comme inattendu, inapproprié ou contestable, continuerait d'être inadmissible⁷⁷. Lorsque la modification du but initial est prévue par la loi, requise par un changement législatif ou légitimée par un autre motif justificatif, le traitement ultérieur devrait aussi être considéré comme compatible avec le but initial⁷⁸.

E. La transparence

Le principe de transparence était dans de nombreux cas limité à la reconnaissabilité de l'art. 4 al. 4 a LPD. Il est repris indirectement à l'art. 6 al. 3 LPD qui prévoit que les données doivent être collectées pour des finalités déterminées et reconnaissables pour la personne concernée. Cette formulation malheureuse n'implique toutefois pas de changements matériels par rapport à l'aLPD, tant la collecte des données que les finalités du traitement doivent être reconnaissables⁷⁹. On considère que la reconnaissabilité est remplie lorsqu'on informe la personne concernée, lorsque les traitements sont prévus par la loi ou lorsqu'ils ressortent clairement des circonstances⁸⁰.

La portée pratique du principe de transparence est fortement réduite puisque l'art. 19 LPD a introduit un devoir d'information systématique pour le responsable du traitement privé⁸¹. La violation du principe de transparence reste une présomption de traitement illicite (art. 30 al. 2 let. a LPD)⁸², mais le non-respect de l'obligation d'information peut désormais être sanctionné par une amende pénale allant jusqu'à CHF 250'000.– pour les

⁷⁶ Cela est également connu du RGPD (art. 6 par. 4 RGPD). Voir également : CR LPD-MEIER/TSCHUMY, art. 6 N 53 ; ROSENTHAL, nDSG, N 35.

⁷⁷ Message nLPD, FF 2017 6644 ss et les références citées.

⁷⁸ CR LPD-MEIER/TSCHUMY, art. 6 N 55 ; SHK DSG-BAERISWYL, art. 6 N 52.

⁷⁹ Message nLPD, FF 2017 6644. Voir également : ROSENTHAL, nDSG, N 33.

⁸⁰ CR LPD-MEIER/TSCHUMY, art. 6 N 42 ss.

⁸¹ Il était précédemment réservé aux données sensibles traitées par les privés et à toutes les données collectées par les organes fédéraux. Cf. *infra* V.B.3.

⁸² Elle peut être justifiée par un motif justificatif de l'art. 31 LPD.

responsables du traitement privés (art. 60 al. 1 let. a LPD) et par une mesure administrative pour les organes fédéraux (art. 51 al. 3 let. c LPD).

F. L'exactitude

Celui qui traite des données personnelles doit s'assurer qu'elles sont exactes (art. 6 al. 5 LPD). Une donnée exacte est une donnée correcte, actuelle et objective⁸³. L'obligation d'exactitude n'est pas absolue, mais elle doit être proportionnée à la finalité du traitement. Certaines obligations légales peuvent même s'opposer à la rectification, à l'effacement, ou à la mise à jour des données⁸⁴.

Il faut donc prendre toutes les mesures appropriées qui permettent de rectifier, d'effacer ou de détruire les données inexactes ou incomplètes au regard des finalités pour lesquelles elles sont collectées ou traitées. Le caractère approprié des mesures dépend notamment du type de traitement, de son étendue, ainsi que du risque que le traitement des données en question présente pour la personnalité et les droits fondamentaux des personnes concernées (art. 6 al. 5 LPD)⁸⁵. Si des données inexactes ne peuvent pas être rectifiées ou complétées, elles doivent alors être effacées ou détruites⁸⁶.

Une donnée inexacte ne doit donc pas être systématiquement détectée et corrigée. Elle doit l'être si elle porte atteinte à la personnalité ou si la personne concernée le demande⁸⁷. Le responsable du traitement n'a pas un devoir de contrôle permanent, mais il doit tenir compte de toutes les modifications dont il a connaissance. Dans le cadre d'une affaire opposant le PFPDT à l'entreprise de renseignements de solvabilité Moneyhouse, le Tribunal administratif fédéral a retenu que si le responsable du traitement doit vérifier que les données qu'il traite sont à jour et que son client a bien un intérêt à connaître la solvabilité d'un tiers, ces vérifications peuvent avoir lieu par sondage. En l'espèce, il suffisait de vérifier 5 % des données communiquées pour s'assurer qu'elles sont exactes et 3 % des demandes pour s'assurer qu'elles sont justifiées⁸⁸.

⁸³ MEIER, Précis, N 745 ; CR LPD-MEIER/TSCHUMY, art. 6 N 66 ; BSK DSG-MAURER-LAMBROU/SCHÖNBÄCHLER, art. 5 N 8.

⁸⁴ Message nLPD, FF 2017 6646 et les références citées.

⁸⁵ CR LPD-MEIER/TSCHUMY, art. 6 N 62 ; SHK DSG-BAERISWYL, art. 6 N 63 ss.

⁸⁶ Message nLPD, FF 2017 6646.

⁸⁷ MEIER, Précis, N 756.

⁸⁸ TAF A-4232/2015 du 18 avril 2017, c. 7.3.2. Pour un résumé de l'arrêt, voir : MÉTILLE/NGUYEN XUAN, pp. 176 ss.

G. La sécurité

La sécurité des données est mentionnée à l'art. 8 LPD qui prévoit que les responsables du traitement et les sous-traitants doivent assurer, par des mesures organisationnelles et techniques appropriées, une sécurité adéquate des données personnelles par rapport au risque encouru. Cette disposition matérialise l'approche fondée sur les risques⁸⁹. Plus le risque d'une atteinte à la sécurité des données est élevé, plus les exigences auxquelles doivent répondre les mesures à prendre seront élevées. Le risque (et donc le besoin de protection) est évalué en tenant compte du type de données traitées et de la finalité, de la nature, de l'étendue et des circonstances du traitement, des causes du risque, des principales menaces, des mesures prises ou prévues pour réduire le risque, de la probabilité et de la gravité d'une violation de la sécurité des données, malgré les mesures prises ou prévues, ainsi que de l'état des connaissances et des coûts de mise en œuvre⁹⁰.

La LPD précise aussi que les mesures doivent permettre d'éviter toute violation de la sécurité des données, soit toute violation de la sécurité entraînant la perte de données personnelles, leur modification, leur effacement ou leur destruction, leur divulgation ou un accès non autorisé à ces données, et ce indépendamment de la question de savoir si la violation est intentionnelle ou non, licite ou illicite (art. 6 et 8 al. 2 LPD).

Les exigences minimales en matière de sécurité des données personnelles figurent dans l'OPDo. Conformément aux art. 2 et 3 OPDo, ces mesures doivent assurer la confidentialité (contrôle de l'accès aux données, contrôle de l'accès aux locaux et aux installations, contrôle d'utilisation)⁹¹, la disponibilité et l'intégrité (contrôle des supports de données, contrôle de la mémoire, contrôle du transport, restauration, disponibilité, fiabilité, intégrité des données, sécurité du système)⁹² et assurer la traçabilité⁹³ (contrôle de la saisie, contrôle de la communication, détection et réparation)⁹⁴.

En cas de traitement automatisé de données sensibles à grande échelle ou de profilage à risque élevé, le responsable du traitement et son sous-traitant doivent établir un règlement de traitement et journaliser les traitements⁹⁵.

⁸⁹ CR LPD-FANTI/STAEGGER, art. 8 N 76 ; PC LPD-BÉGUIN, art. 8 N 5 ; Message nLPD, FF 2017 6650. L'art. 2 OPDo parle du « besoin de protection ».

⁹⁰ Art 1 OPDo.

⁹¹ CR LPD-FANTI/STAEGGER, art. 8 N 129 ss.

⁹² CR LPD-FANTI/STAEGGER, art. 8 N 141 ss.

⁹³ On utilise parfois le terme « authentification » (PC LPD-BÉGUIN, art. 8 N 7).

⁹⁴ CR LPD-FANTI/STAEGGER, art. 8 N 170 ss ; SHK DSG-BAERISWYL, art. 8 N 55.

⁹⁵ CR LPD-FANTI/STAEGGER, art. 8 N 183 et 199.

Le règlement doit notamment comprendre des informations sur l'organisation interne, sur les procédures de traitement et de contrôle des données, ainsi que sur les mesures visant à garantir la sécurité des données (art. 5 OPDo). Quant à la journalisation, elle doit indiquer au moins l'enregistrement, la modification, la lecture, la communication, l'effacement et la destruction des données (art. 4 al. 1 OPDo)⁹⁶. Une telle mesure ne serait pas nécessaire si des mesures préventives suffisent à garantir la protection des données, ce qui semble illusoire puisque la journalisation est notamment nécessaire lorsque, sans cette mesure, il n'est pas possible de vérifier *a posteriori* que les données ont été traitées conformément aux finalités pour lesquelles elles ont été collectées ou communiquées.

Les procès-verbaux de journalisation doivent être conservés durant au moins un an, séparément du système dans lequel les données personnelles sont traitées et n'être accessibles que de manière limitée. Ils doivent fournir des informations sur l'identité de la personne qui a effectué le traitement, la nature, la date et l'heure du traitement et, cas échéant, l'identité du destinataire des données (art. 4 al. 4 et 5 OPDo). Cette exigence risque d'être compliquée et coûteuse à mettre en place pour beaucoup de responsables du traitement⁹⁷.

La sécurité est à la fois un principe et une obligation du responsable du traitement et du sous-traitant. Ainsi, l'art. 61 let. c LPD prévoit que les personnes privées qui, intentionnellement, ne respectent pas les exigences minimales en matière de sécurité des données prévues dans l'OPDo s'exposent à une amende pénale de CHF 250'000.-.

V. Quelles sont les obligations du responsable du traitement ?

A. Les obligations déjà connues de l'aLPD

1. Le transfert à l'étranger

L'exigence de l'aLPD selon laquelle aucune donnée personnelle ne pouvait être transmise à l'étranger si la personnalité des personnes concernées devait s'en trouver gravement menacée a été supprimée, car elle créait trop d'insécurité juridiques⁹⁸.

⁹⁶ Pour les données personnelles généralement accessibles au public, il suffit de journaliser l'enregistrement, la modification, l'effacement et la destruction des données (art. 4 al. 3 OPDo).

⁹⁷ CR LPD-FANTI/STAEGGER, art. 8 N 193 ; SHK DSG-BAERISWYL, art. 8 N 56.

⁹⁸ Message nLPD, FF 2017 6657.

La condition est désormais que des données personnelles peuvent être communiquées à l'étranger si le Conseil fédéral a constaté que l'Etat concerné dispose d'une législation assurant un niveau de protection adéquat (art. 16 al. 1 LPD)⁹⁹. La liste des Etats assurant un niveau de protection adéquat figure à l'Annexe 1 de l'OPDo. Dès qu'un Etat figure dans la liste, la libre circulation des données personnelles de la Suisse vers cet Etat est garantie, sans autre mesure de vérification du responsable du traitement¹⁰⁰.

En l'absence d'une décision du Conseil fédéral, des données personnelles peuvent être communiquées à l'étranger si un niveau de protection approprié est garanti par d'autres moyens (art. 16 al. 2 LPD)¹⁰¹ ou si une dérogation s'applique (art. 17 LPD)¹⁰². Un niveau de protection adéquat peut en particulier être garanti par un traité international (art. 16 al. 2 let. a LPD) ou des clauses contractuelles (clauses contractuelles¹⁰³ entre l'exportateur des données et le destinataire à l'étranger ou des règles d'entreprise contraignantes)¹⁰⁴. On soulignera toutefois que les garanties contractuelles ne peuvent pas déroger au droit impératif de l'Etat de destination, et que dans certains cas, aucun engagement contractuel ne pourra garantir un niveau de protection suffisant¹⁰⁵.

Les dérogations (art. 17 LPD) concernent d'autres situations dans lesquelles une communication dans un Etat n'assurant pas un niveau de protection adéquat est possible¹⁰⁶. C'est en particulier le cas lorsque la personne concernée a expressément donné son consentement à la communication, après avoir été informée de l'Etat en question et des risques du transfert dans cet Etat, ou si la communication est en relation directe avec la conclusion ou l'exécution d'un contrat, non seulement entre le responsable du traitement et la personne concernée, mais aussi entre le responsable du traitement et son cocontractant, dans l'intérêt de la personne concernée (art. 17 al. 1 let. a et b LPD)¹⁰⁷.

⁹⁹ CR LPD-FISCHER, Intro. aux art. 16-18 N 15 ss ; ROSENTHAL, nDSG, N 64 ss.

¹⁰⁰ Message nLPD, FF 2017 6657 ss.

¹⁰¹ ROSENTHAL, nDSG, N 71 ss.

¹⁰² ROSENTHAL, nDSG, N 75 ss.

¹⁰³ Des clauses types de protection des données préalablement approuvées par le PFPDT (art. 16 al. 2 let. d LPD), un contrat entre le responsable du traitement (ou le sous-traitant) et son cocontractant à l'étranger préalablement communiquées au PFPDT (art. 16 al. 2 let. b LPD), ou des garanties spécifiques élaborées par l'organe fédéral et préalablement communiquées au PFPDT (art. 16 al. 2 let. c LPD). Voir également PFPDT, Transfert de données personnelles.

¹⁰⁴ Des règles d'entreprise contraignantes préalablement approuvées par le PFPDT ou son homologue dans un Etat assurant un niveau de protection adéquat (art. 16 al. 2 let. e LPD).

¹⁰⁵ CR LPD-FISCHER, art. 16 N 63 et 95 ss. Voir aussi : CJUE, C-311/18, ECLI:EU:C:2020:559, (Maximilian Schrems et Data Protection Commissioner/Facebook Ireland Ltd).

¹⁰⁶ CR LPD-FISCHER, art. 17 N 2.

¹⁰⁷ Message nLPD, FF 2017 6661.

C'est également le cas lorsque la communication est nécessaire à la sauvegarde d'un intérêt public prépondérant, à la constatation, à l'exercice ou à la défense d'un droit devant un tribunal ou une autre autorité étrangère (art. 17 al. 2 let. c LPD), ou pour protéger la vie ou l'intégrité corporelle de la personne concernée ou d'un tiers (art. 17 al. 2 let. d LPD)¹⁰⁸. C'est finalement aussi le cas si la personne concernée a rendu les données personnelles accessibles à tout un chacun et ne s'est pas opposée expressément au traitement (art. 17 al. 2 let. e LPD) ou si les données proviennent d'un registre prévu par la loi et destiné à fournir des informations au public (art. 17 al. 2 let. f LPD)¹⁰⁹.

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

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

2. La sous-traitance

Le responsable du traitement peut recourir à des sous-traitants pour effectuer certaines opérations. Les traitements au sein d'une même personne juridique (succursale, unité administrative, employé) ne constituent en principe pas des cas de sous-traitance¹¹⁰.

L'art. 9 LPD reprend en substance les mêmes conditions que celles de l'ancien droit, à savoir que le responsable du traitement peut confier le traitement de données personnelles à un sous-traitant si la loi ou un contrat le prévoit (art. 9 al. 1 LPD). L'exigence d'avoir un contrat est une obligation qui repose tant sur le responsable du traitement que sur le sous-traitant.

Le sous-traitant ne peut effectuer que les traitements que le responsable du traitement est en droit d'effectuer lui-même (art. 9 al. 1 let. a LPD), et toute obligation légale ou contractuelle de garder le secret doit être respectée (art. 9 al. 1 let. b LPD). Le consentement de la personne concernée n'est pas nécessaire¹¹¹, mais la personne concernée

¹⁰⁸ Seulement s'il n'est pas possible d'obtenir le consentement de la personne concernée dans un délai raisonnable (CR LPD-FISCHER, art. 17 N 45)

¹⁰⁹ Seulement s'il est accessible au public ou à toute personne justifiant d'un intérêt légitime et pour autant que les conditions légales pour la consultation dans le cas d'espèce soient remplies (CR LPD-FISCHER, art. 17 N 57).

¹¹⁰ Message nLPD, FF 2017 6652.

¹¹¹ Dans le même sens : ROSENTHAL, nDSG, N 57.

doit être informée de l'existence de destinataires (ou catégories de destinataires), parmi lesquels figurent les sous-traitants (art. 19 al. 2 let. c LPD).

L'art. 9 al. 3 LPD est nouveau et prévoit une interdiction pour le sous-traitant de sous-traiter à son tour (délégation de deuxième rang) sans avoir l'autorisation préalable du responsable du traitement. C'est une petite nouveauté, l'aLPD n'étant pas claire à cet égard. L'autorisation peut être spécifique ou générale¹¹². Si l'autorisation est générale, le sous-traitant informe le responsable du traitement lorsqu'il envisage de recourir à d'autres tiers ou de les remplacer. Le responsable du traitement peut s'opposer à cette modification (art. 7 al. 2 OPDo). La loi n'indiquant pas les conséquences éventuelles de cette opposition, il serait bienvenu de préciser par contrat si cela donne des droits de résiliation ou modification du contrat.

Comme dans l'ancien droit, la sous-traitance des données personnelles qui sont protégées par un secret n'est pas exclue, mais les conditions particulières applicables au secret concerné doivent être respectées. Par exemple dans le cas du secret professionnel, pour que la sous-traitance soit possible, le sous-traitant devra pouvoir être qualifié d'auxiliaire au sens de l'art. 321 CP¹¹³.

Le responsable du traitement a donc un devoir de diligence dans le but de sauvegarder les droits des personnes concernées. Il doit s'assurer de manière active que le sous-traitant respecte la loi dans la même mesure que lui. Cela concerne non seulement les règles relatives à la sécurité, mais aussi le respect des principes généraux de protection des données. Par analogie avec l'art. 55 CO, il doit mettre tout en œuvre pour éviter d'éventuelles violations de la LPD. Il doit ainsi veiller à choisir soigneusement son mandataire (*curia in eligendo*), à lui donner les instructions adéquates (*curia in instruendo*) et à exercer la surveillance nécessaire (*curia in custodiendo*)¹¹⁴.

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

3. Le conseiller à la protection des données

Le conseiller à la protection des données figure désormais dans la loi, mais de manière limitée. L'art. 10 LPD constate simplement que les responsables du traitement privés peuvent nommer un conseiller à la protection des données. Il s'agit toujours d'une faculté

¹¹² CR LPD-MÉTILLE, art. 9 N 83 ; SHK DSG-BAERISWYL, art. 9 N 60.

¹¹³ CR LPD-MÉTILLE, art. 9 N 59 ; SHK DSG-BAERISWYL, art. 9 N 53.

¹¹⁴ CR LPD-MÉTILLE, art. 9 N 71.

et en aucun cas d'une obligation¹¹⁵. C'est en revanche une obligation pour les organes fédéraux, comme précédemment (art. 10 al. 4 LPD)¹¹⁶.

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

Le seul bénéfice légal de la désignation d'un conseiller est que le responsable du traitement peut renoncer à consulter le PFPDT lorsque l'analyse d'impact a révélé que le traitement présente encore un risque élevé malgré les mesures prévues par le responsable du traitement pour atténuer ce risque, à la condition d'avoir consulté son conseiller (art. 10 al. 3 et art. 23 al. 4 LPD)¹¹⁷.

Pour bénéficier de cet allègement (art. 10 al. 3 LPD), il faut que le conseiller exerce sa fonction de manière indépendante par rapport au responsable du traitement et sans recevoir d'instruction de celui-ci (let. a), qu'il n'exerce pas de tâches incompatibles avec ses tâches de conseiller (let. b), qu'il dispose des connaissances professionnelles nécessaires (let. c), et que le responsable du traitement ait publié les coordonnées du conseiller et les ait communiquées au PFPDT (let. d).

Le conseiller peut être interne ou externe. Si c'est un collaborateur, son indépendance doit être garantie par la hiérarchie en place dans l'entreprise en le subordonnant en principe directement à la direction du responsable du traitement¹¹⁸. L'interdiction d'exercer des tâches incompatibles empêchera en principe qu'il soit membre de la direction, qu'il exerce des fonctions dans les domaines de la conduite du personnel ou de la gestion des systèmes informatiques, ou qu'il appartienne à un service qui traite des données personnelles sensibles¹¹⁹. Les fonctions de conseiller à la protection des données et de délégué à la sécurité de l'information ne semblent en revanche pas incompatibles pour le Conseil fédéral¹²⁰.

¹¹⁵ CR LPD-FISCHER, art. 10 N 16 ; Message nLPD, FF 2017 6652 ; GILLIÉRON, Conseiller, registre et analyse, p. 128.

¹¹⁶ Cette obligation est reprise dans l'ordonnance aux art. 25 ss OPDo.

¹¹⁷ Pour le surplus, l'intérêt à nommer un conseiller pour les entreprises est relativement faible (CR LPD-FISCHER, art. 10 N 22 et 40 ss ; GILLIÉRON, Conseiller, registre et analyse, p. 130).

¹¹⁸ CR LPD-FISCHER, art. 10 N 44 ss.

¹¹⁹ CR LPD-FISCHER, art. 10 N 49 ss ; GILLIÉRON, Conseiller, registre et analyse, p. 129.

¹²⁰ Message nLPD, FF 2017 6652 ss.

B. Les nouvelles obligations

1. Le registre des activités de traitement

L'obligation prévue par l'art. 11a aLPD de déclarer certains fichiers a été remplacée par une obligation de tenir un registre des activités de traitement (art 12 LPD)¹²¹. Cette obligation s'applique à tous les responsables du traitement et les sous-traitants qui emploient au moins 250 collaborateurs au 1^{er} janvier d'une année (art. 12 al. 5 LPD et 24 OPDo). Pour les personnes physiques et les entreprises de moins de 250 collaborateurs, l'obligation ne s'applique qu'en cas de traitement de données sensibles à grande échelle ou de profilage à risque élevé (art. 24 OPDo).

Le PFPDT peut avoir accès au registre des responsables du traitement privés sur demande, mais pas les personnes concernées. En revanche, le registre des organes fédéraux est publiquement accessible (art. 56 LPD).

Le registre n'est ni une copie des données personnelles traitées, ni un journal détaillé des traitements¹²². C'est un descriptif général des activités de traitement qui permet d'avoir une vue d'ensemble de tous les traitements et de se faire rapidement une idée sur la conformité des traitements. Son contenu correspond dans une large mesure aux indications que la personne concernée doit recevoir en vertu du devoir d'information et du droit d'accès¹²³.

L'art. 12 al. 2 LPD précise les indications minimales que doit contenir le registre du responsable du traitement : l'identité (le nom) du responsable du traitement (let. a), la finalité du traitement (let. b), une description des catégories des personnes concernées et des catégories de données personnelles traitées (let. c), les catégories des destinataires auxquels les données sont susceptibles d'être communiquées (let. d), le délai de conservation des données personnelles ou les critères selon lesquels ce délai est fixé (let. e), si possible une description générale des mesures de sécurité (let. f), et en cas de communication à l'étranger, le nom de l'Etat en question et les garanties prises selon l'art. 16 al. 2 LPD (let. g). Il n'y a pas d'exigence de forme¹²⁴.

Le registre du sous-traitant doit contenir l'identité du sous-traitant et du responsable du traitement, les catégories de traitements effectués pour le compte du responsable du traitement, si possible une description générale des mesures de sécurité, et en cas de

¹²¹ Un tel registre est également prévu par l'art. 30 RGPD.

¹²² Message nLPD, FF 2017 6655.

¹²³ CR LPD-GILLIÉRON, art. 12 N 16 ; Message nLPD, FF 2017 6652 ss.

¹²⁴ Dans le même sens : ROSENTHAL, nDSG, N 145.

communication à l'étranger, le nom de l'Etat en question et les garanties prises selon l'art. 21 al. 2 LPD¹²⁵.

Le nom du responsable du traitement et la finalité n'appellent pas de commentaires particuliers. Les catégories des personnes concernées s'entendent comme des groupes partageant les mêmes caractéristiques¹²⁶. Il en va de même pour les catégories des destinataires¹²⁷. Quant aux catégories des données traitées, elles doivent permettre de savoir quels types de données sont traitées sans que la donnée elle-même ne doive être indiquée¹²⁸.

La description générale des mesures visant à garantir la sécurité des données devrait faire apparaître d'éventuels manquements dans les mesures de sécurité. Elle n'est obligatoire que si les mesures peuvent être définies de manière suffisamment concrète¹²⁹.

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

La LPD introduit l'analyse d'impact relative à la protection des données (art. 22 LPD)¹³⁰. Il s'agit d'un outil préventif à destination du responsable du traitement qui devrait lui permettre, après avoir décrit le traitement qu'il entend mettre en œuvre, d'en évaluer la nécessité et la proportionnalité tout en évaluant les risques pesant sur les droits et libertés des personnes physiques au vu du traitement envisagé. En cas de risque, le responsable du traitement doit déterminer les mesures nécessaires pour y faire face¹³¹. L'analyse d'impact relative à la protection des données personnelles doit être conservée pendant au moins deux ans après la fin du traitement des données (art. 14 OPDo).

Une analyse d'impact n'est requise que lorsque le traitement envisagé est susceptible d'entraîner un risque élevé pour la personnalité ou les droits fondamentaux de la personne

¹²⁵ Art. 12 al. 3 LPD.

¹²⁶ Par exemple des clients, des employés, des abonnés, des concurrents, etc. (GILLIÉRON, Conseiller, registre et analyse, p. 134).

¹²⁷ Par exemple des sous-traitants, des autorités de surveillance, des entreprises appartenant au même groupe, etc. (GILLIÉRON, Conseiller, registre et analyse, p. 134).

¹²⁸ CR LPD-GILLIÉRON, art. 12 N 31 ss ; par exemple le nom, le prénom, l'adresse, la langue de correspondance, les données relatives aux achats, les préférences publicitaires, etc.

¹²⁹ CR LPD-GILLIÉRON, art. 12 N 34 ; Message nLPD, FF 2017 6655 ; GILLIÉRON, Conseiller, registre et analyse, p. 135.

¹³⁰ Cette obligation est également connue du droit européen (art. 35 RGPD). Voir également : COMITÉ EUROPÉEN DE LA PROTECTION DES DONNÉES, pp. 1 ss ; GROUPE DE TRAVAIL « ARTICLE 29 » SUR LA PROTECTION DES DONNÉES, pp. 1 ss.

¹³¹ CR LPD-GILLIÉRON, art. 22 N 23 ; GILLIÉRON, Conseiller, registre et analyse, p. 140 ; Message nLPD, FF 2017 6676 ; SHK DSG-BLONSKI, art. 22 N 1.

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

La notion de risque élevé est complexe et floue. Dans son Aide-mémoire concernant l'analyse d'impact relative à la protection des données personnelles (AIPD) au sens des art. 22 et 23 LPD, le PFPDT considère que la notion de risque élevé est une notion juridique indéterminée qui se précisera au fil de la pratique et de la jurisprudence¹³². Le risque dépend notamment de la nature, de l'étendue, des circonstances, de la finalité du traitement et du type de technologies utilisées. De manière logique, il y a lieu de conclure à un risque élevé selon si le traitement est étendu, selon le caractère sensible des données ou encore si la finalité du traitement est vaste¹³³. Cette liste n'est pas exhaustive et il appartient au responsable du traitement d'évaluer l'opportunité de réaliser une telle analyse d'impact, préalablement à tout traitement¹³⁴.

Le PFPDT considère toutefois qu'il y a un facteur de risque absolu dans les cas mentionnés à l'art. 22 al. 2 LPD, soit lorsque le responsable du traitement traite des données sensibles à grande échelle (let. a) ou lorsque le responsable du traitement opère une surveillance systématique de grandes parties du domaine public (let. b)¹³⁵. Il retient des facteurs de risque notoires s'il y a un profilage à risque élevé, une décision individuelle automatisée, le recours à de nouvelles technologies (y compris l'intelligence artificielle), une collecte secrète de données, un volume important de données ou de personnes, une longue durée ou une couverture géographique importante, une interconnexion ou une comparaison de différentes bases de données, une communication à des tiers, une surveillance de personnes ou un empêchement d'exercer un droit, d'utiliser un service ou d'exécuter un contrat¹³⁶. Dans les deux cas, il faut réaliser une analyse d'impact si l'un de ces facteurs de risque est réalisé.

¹³² PFPDT, Aide-mémoire, p. 5.

¹³³ Sauf cas exceptionnels, on imagine difficilement qu'un traitement isolé puisse entraîner un risque élevé (CR LPD-GILLIÉRON, art. 22 N 25) ; Message nLPD, FF 2017 6676.

¹³⁴ GILLIÉRON, Conseiller, registre et analyse, p. 145.

¹³⁵ PFPDT, Aide-mémoire, pp. 6 ss ; GILLIÉRON, Conseiller, registre et analyse, p. 140.

¹³⁶ PFPDT, Aide-mémoire, pp. 6 ss.

Bien qu'il s'agisse d'une obligation, sa violation n'est pas sanctionnée pénalement. Le PFPDT peut toutefois ordonner à la personne privée ou à l'organe fédéral dans le cadre d'une enquête d'en établir une (art. 51 al. 3 let. d LPD).

L'art. 22 al. 3 LPD prévoit ce que doit contenir une analyse d'impact, à savoir une description du traitement envisagé, une évaluation des risques pour la personnalité ou les droits fondamentaux de la personne concernée, ainsi que les mesures prévues pour protéger sa personnalité et ses droits fondamentaux. Autrement dit, l'analyse d'impact doit contenir une étude du contexte et des enjeux du traitement envisagé, des mesures prévues, des risques liés à la sécurité des données, de leur impact sur la vie privée ainsi qu'une phase de validation et de suivi. Il s'agit en somme d'un inventaire des risques et des mesures potentiellement applicables¹³⁷. Si la LPD ne contient pas de méthodologie à adopter pour réaliser une analyse d'impact, il est possible de s'inspirer de l'Annexe 2 de l'aide-mémoire établi par le PFPDT¹³⁸.

3. L'information

Le devoir d'informer lors de la collecte de données personnelles (art. 19 LPD) vient renforcer le principe de transparence¹³⁹. Il s'applique autant lorsque les données sont collectées directement auprès de la personne concernée ou auprès d'un tiers (art. 19 al. 1 LPD). Dans ce dernier cas, le responsable du traitement doit informer la personne concernée au plus tard un mois après avoir obtenu les données, voire au moment de la communication des données s'il les communique avant l'échéance de ce délai d'un mois (art. 19 al. 5 LPD).

Le devoir d'informer n'est pas absolu et la LPD prévoit des cas où l'obligation d'informer tombe complètement (art. 20 al. 1 et 2 LPD) et des cas où le devoir d'informer peut être limité sur la base d'une pesée d'intérêts (art. 20 al. 3 LPD)¹⁴⁰. Les motifs justificatifs de l'art. 31 LPD ne sont en revanche pas applicables¹⁴¹.

Il n'y a ainsi pas de devoir d'informer lorsque la personne concernée a déjà reçu les informations (art. 20 al. 1 let. a LPD). Cela peut être le cas parce qu'elle avait été informée antérieurement et que les informations n'ont pas changé depuis, ou parce que la personne concernée a déjà reçu les informations en vue de son consentement à un traitement de données, par exemple par le biais de conditions générales liées à un service¹⁴². Le Conseil

¹³⁷ CR LPD-GILLIÉRON, art. 22 N 53 ss.

¹³⁸ PFPDT, Aide-mémoire, pp. 13 ss.

¹³⁹ CR LPD-FLUECKIGER, Intro. aux art. 19 à 21 N 2 ; RAEDLER, Information, p. 83.

¹⁴⁰ Sur les différentes exceptions : RAEDLER, Information, pp. 107 ss.

¹⁴¹ Dans le même sens, ROSENTHAL, nDSG, N 92 ; CR LPD-FLUECKIGER art. 20 N 11.

¹⁴² RAEDLER, Information, p. 107.

fédéral considère que c'est aussi le cas quand la personne a elle-même communiqué des données sans intervention du responsable du traitement, par exemple lors de la remise d'un dossier de candidature¹⁴³. Si l'on comprend bien que le responsable du traitement ne pouvait pas informer avant de recevoir le dossier, la protection de la bonne foi exige néanmoins qu'il informe sur tous les éléments que la personne concernée ne pouvait pas raisonnablement envisager¹⁴⁴.

Il n'y a pas non plus d'obligation d'informer lorsque la loi prévoit le traitement des données (art. 20 al. 1 let. b LPD)¹⁴⁵, qu'il soit obligatoire ou envisagé, ou si le responsable du traitement est une personne privée liée par une obligation légale de garder le secret (art. 20 al. 1 let. c LPD), car on estime que l'obligation légale de confidentialité prime sur le devoir d'information¹⁴⁶. Les médias à caractère périodique bénéficient également, à certaines conditions, d'une exception pour les données traitées exclusivement pour la publication dans la partie rédactionnelle (art. 20 al. 1 let. d LPD)¹⁴⁷.

Il n'y a finalement pas d'obligation d'informer lorsque l'information est impossible à donner ou nécessiterait des efforts disproportionnés et que les données personnelles ne sont pas collectées auprès de la personne concernée (art. 20 al. 2 LPD). L'information est considérée comme impossible lorsque la personne concernée n'est pas identifiable malgré un certain nombre de recherches¹⁴⁸. Quant aux efforts disproportionnés, ils le sont lorsqu'ils paraissent injustifiés par rapport au bénéfice que la personne concernée retirerait de l'information¹⁴⁹. Ces exceptions s'appliquent restrictivement¹⁵⁰.

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

¹⁴³ Message nLPD, FF 2017 6671.

¹⁴⁴ CR LPD-FLUECKIGER, art. 20 N 4.

¹⁴⁵ Ce qui revient à dire que l'obligation d'informer des organes fédéraux est limitée (dans le même sens : ROSENTHAL, nDSG, N 103).

¹⁴⁶ CR LPD-FLUECKIGER, art. 20 N 9 ; Message nLPD, FF 2017 6671.

¹⁴⁷ Dans le cas où l'information fournirait des indications sur les sources d'information, qu'il en résulterait un droit de regard sur des projets de publication ou que la libre formation de l'opinion publique serait compromise (art. 27 LPD).

¹⁴⁸ Par exemple en présence de la photo d'un inconnu (RAEDLER, Information, p. 108).

¹⁴⁹ Par exemple l'archivage d'intérêt public qui concerne un grand nombre de personnes sans pour autant disposer d'un réel intérêt compte tenu de l'ancienneté des données (Message nLPD, FF 2017 6672 ; CR LPD-FLUECKIGER, art. 20 N 13 ; RAEDLER, Information, p. 108).

¹⁵⁰ Message nLPD, FF 2017 6671 ; PC LPD-JACCOUD/FANTI/STAEGGER, art. 20 N 30.

La limitation de l'information prévue par l'art. 20 al. 3 LPD requiert une pesée d'intérêt et permet, selon les cas de renoncer, restreindre ou différer l'information. La liste des cas de limitation est exhaustive et la disposition doit être interprétée restrictivement¹⁵¹. Le principe de proportionnalité s'applique et l'on choisira, de manière générale, la solution la plus favorable à la personne concernée, garantissant la transparence maximale du traitement compte tenu des circonstances¹⁵².

Le premier cas de limitation est justifié par les intérêts prépondérants d'un tiers (art. 20 al. 3 let. a LPD). Le deuxième cas vise des situations particulières où le fait d'informer la personne concernée empêche totalement le traitement d'atteindre son but principal (art. 20 al. 3 let. b LPD). Il ne suffit pas que l'absence d'information soit plus pratique pour le responsable du traitement ou qu'elle soit justifiée par des intérêts purement économiques¹⁵³. Le troisième cas prend en compte les intérêts prépondérants du responsable du traitement privé (art. 20 al. 3 let. c LPD)¹⁵⁴, à la condition qu'il ne communique pas les données à des tiers (responsables du traitement). La communication de données entre des entreprises contrôlées par une même personne morale n'est pas considérée comme une communication à des tiers en application de cette disposition (art. 20 al. 4 LPD).

La loi ne précise pas la manière de fournir l'information, mais la personne concernée doit l'obtenir sans avoir à la demander. L'OPDo précise que le responsable du traitement doit communiquer aux personnes concernées les informations sur la collecte de données personnelles de manière concise, transparente, compréhensible et facilement accessible (art. 13 OPDo)¹⁵⁵. Il ne doit pas s'assurer que la personne concernée en a effectivement pris connaissance. Une information générale sous forme de conditions générales, de déclaration de confidentialité sur un site web ou des pictogrammes¹⁵⁶ est admissible si elle contient tous les éléments nécessaires¹⁵⁷.

¹⁵¹ CR LPD-FLUECKIGER, art. 20 N 18 ; Message nLPD, FF 2017 6672 ; RAEDLER, Information, p. 110.

¹⁵² Message nLPD, FF 2017 6672.

¹⁵³ Message nLPD, FF 2017 6673. Sur la forme de l'information, voir notamment : ROSENTHAL, nDSG, N 99.

¹⁵⁴ Lorsque le responsable du traitement est un organe fédéral, l'exception s'applique s'il y a un intérêt public prépondérant, en particulier la sûreté intérieure ou extérieure de la Suisse, ou si la communication des informations est susceptible de compromettre une enquête, une instruction ou une procédure judiciaire ou administrative (art. 20 al. 3 let. d LPD).

¹⁵⁵ Si le responsable du traitement restreint ou diffère la communication au sens de l'al. 3, il conviendrait d'appliquer l'art. 18 OPDo par analogie (RAEDLER, Information, p. 110).

¹⁵⁶ Voir par exemple THOUVENIN *et al.*, N 1 ss ; RAEDLER, Information, p. 104.

¹⁵⁷ CR LPD-FLUECKIGER, art. 19 N 17 ; Message nLPD, FF 2017 6668.

Le responsable du traitement doit donc communiquer à la personne concernée toutes les informations nécessaires pour qu'elle puisse faire valoir ses droits selon la LPD et pour garantir la transparence des traitements¹⁵⁸. L'art. 19 al. 2 LPD dresse la liste des informations minimales à communiquer, soit l'identité et les coordonnées du responsable du traitement, la finalité du traitement, les destinataires ou les catégories de destinataires¹⁵⁹ si les données personnelles leur sont transmises, les pays ou organismes internationaux concernés et les garanties prévues¹⁶⁰ s'il y a un transfert à l'étranger, ainsi que les catégories de données traitées si les données personnelles ne sont pas collectées auprès de la personne concernée.

Contrairement à ce qui est prévu en droit européen, il n'y a pas d'obligation d'indiquer les droits de la personne concernée ou la durée de conservation des données¹⁶¹.

Si la violation du principe de transparence reste une présomption de traitement illicite (art. 30 al. 2 let. a LPD)¹⁶², le non-respect de l'obligation d'information peut désormais être sanctionné par une amende pénale allant jusqu'à CHF 250'000.- pour les responsables du traitement privés¹⁶³.

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

La violation de la sécurité des données est définie comme toute violation de la sécurité entraînant de manière accidentelle ou illicite la perte de données personnelles, leur modification, leur effacement ou leur destruction, leur divulgation ou un accès non autorisé à ces données (art. 5 let. h LPD). La violation peut être causée par un tiers, mais son auteur peut aussi être un collaborateur qui outrepassé ses compétences ou qui fait preuve de négligence, voire une défaillance technique¹⁶⁴. La violation de la sécurité des données peut entraîner une perte de contrôle de la personne concernée sur ses données ou une utilisation abusive de celles-ci. Elle peut aussi engendrer une violation de la confidentialité, par exemple en entraînant la divulgation d'informations que la personne concernée souhaitait garder secrètes¹⁶⁵.

¹⁵⁸ CR LPD-FLUECKIGER, art. 19 N 35.

¹⁵⁹ Cela inclut tant les sous-traitants que les tiers (CR LPD-FLUECKIGER, art. 19 N 43 ; RAEDLER, Information, pp. 102 ss).

¹⁶⁰ Des garanties sont nécessaires en cas de transfert vers un pays qui n'est pas considéré comme adéquat au sens de l'art. 16 al. 1 LPD. Si le transfert est justifié par une dérogation de l'art. 17 LPD, elle doit aussi être indiquée.

¹⁶¹ CR LPD-FLUECKIGER, art. 19 N 47 ss ; RAEDLER, Information, p. 103.

¹⁶² Elle peut être justifiée par un motif justificatif de l'art. 31 LPD.

¹⁶³ Art. 60 al. 1 LPD. Par une mesure administrative pour les organes fédéraux (art. 51 al. 3 LPD).

¹⁶⁴ CR LPD-MÉTILLE/MEYER, art. 24 N 30.

¹⁶⁵ Message nLPD, FF 2017 6680 ss.

Si la violation de la sécurité des données entraîne vraisemblablement un risque élevé pour la personnalité ou les droits fondamentaux de la personne concernée, le responsable du traitement doit l'annoncer dans les meilleurs délais au PFPDT (art. 24 al. 1 LPD)¹⁶⁶. Plus le risque est élevé et le nombre de personnes concernées important, plus l'annonce doit intervenir rapidement¹⁶⁷. De plus, à la demande du PFPDT ou si cela est nécessaire à la protection de la personne concernée, le responsable du traitement doit également informer cette dernière (art. 24 al. 4 LPD). L'information à la personne concernée devrait toujours intervenir lorsque cela lui permet de réduire les risques en prenant des dispositions pour se protéger, comme la modification de mots de passe¹⁶⁸.

L'annonce doit indiquer au minimum la nature de la violation (effacement ou destruction de données, leur perte, leur modification ou leur communication à des tiers non autorisés), les conséquences, y compris les risques éventuels, pour les personnes concernées, le moment et la durée (dans la mesure du possible), les catégories et le nombre approximatif de données personnelles concernées (dans la mesure du possible), les catégories et le nombre approximatif de personnes concernées (dans la mesure du possible), et les mesures prises ou envisagées pour remédier à la situation ou pour atténuer ses conséquences, y compris les risques éventuels, ainsi que le nom et les coordonnées d'une personne de contact (art. 24 al. 2 LPD et 15 al. 1 OPDo)¹⁶⁹. Le responsable du traitement peut compléter ultérieurement son annonce s'il n'a pas toutes les informations (art. 15 al. 2 OPDo).

Le PFPDT recommande d'utiliser son service d'annonce en ligne des violations de la sécurité des données¹⁷⁰. Le responsable du traitement reste libre d'utiliser un autre moyen, par exemple par courrier¹⁷¹.

Si la violation de la sécurité des données s'est produite chez le sous-traitant, il ne doit pas l'annoncer au PFPDT, mais informer dans les meilleurs délais le responsable du traitement (art. 24 al. 3 LPD). L'annonce est ici due pour toute violation, sans qu'il soit nécessaire qu'elle entraîne un risque élevé¹⁷².

Le responsable du traitement peut restreindre l'information à la personne concernée, la différer ou y renoncer dans certains cas (art. 24 al. 5 LPD), mais pas l'information au PFPDT. C'est en particulier le cas si les intérêts prépondérants d'un tiers l'exigent, si un

¹⁶⁶ Pour une liste d'exemples de violations nécessitant ou non une annonce, voir : CR LPD-MÉTILLE/MEYER, art. 24 N 44 ss.

¹⁶⁷ Message nLPD, FF 2017 6681 ; RAEDLER, Information, p. 121.

¹⁶⁸ CR LPD-MÉTILLE/MEYER, art. 24 N 69 ; RAEDLER, Information, p. 119.

¹⁶⁹ Message nLPD, FF 2017 6681.

¹⁷⁰ Disponible à l'adresse : <https://databreach.edoeb.admin.ch/report>.

¹⁷¹ CR LPD-MÉTILLE/MEYER, art. 24 N 53.

¹⁷² CR LPD-MÉTILLE/MEYER, art. 24 N 92.

devoir légal de garder le secret l'interdit, ou si le devoir d'informer est impossible à respecter ou nécessite des efforts disproportionnés¹⁷³. On considère que le devoir d'informer est réputé impossible à respecter lorsque le responsable du traitement n'est pas en mesure d'identifier les personnes concernées par la violation de la sécurité des données¹⁷⁴. On estime que l'information nécessite des efforts disproportionnés dès lors qu'il faudrait informer individuellement un grand nombre de personnes concernées et que les coûts qui en résulteraient semblent excessifs au regard du gain qu'en retireraient les personnes concernées¹⁷⁵.

Le responsable du traitement peut aussi choisir d'informer la personne concernée par une communication publique, à la condition que l'information des personnes concernées soit garantie de manière équivalente¹⁷⁶. On estime que cette condition est remplie quand une annonce individuelle ne permettrait pas d'améliorer sensiblement l'information de la personne concernée¹⁷⁷.

5. Le représentant

Le responsable du traitement privé qui a son siège ou son domicile à l'étranger et traite des données personnelles concernant des personnes en Suisse doit désigner un représentant en Suisse lorsque l'une des cinq conditions suivantes est remplie (art. 14 al. 1 LPD)¹⁷⁸ : le traitement est en rapport avec une offre de biens ou de services en Suisse (let. a), le traitement est en rapport avec un suivi du comportement de ces personnes en Suisse (let. a), il s'agit d'un traitement de données personnelles à grande échelle (let. b), il s'agit d'un traitement régulier de données personnelles (let. c), ou le traitement présente un risque élevé pour la personnalité des personnes concernées (let. d). Cette obligation a été introduite par le Parlement¹⁷⁹.

Le responsable du traitement doit évidemment publier le nom et l'adresse de son représentant (art. 14 al. 3 LPD), mais un enregistrement auprès du PFPDT n'est étonnamment pas prévu par la loi¹⁸⁰. Il sert de point de contact pour les personnes concernées et le PFPDT (art. 14 al. 2 LPD). Conformément à l'art. 15 al. 1 LPD, le représentant doit en particulier tenir un registre des activités de traitement du responsable

¹⁷³ On notera qu'un intérêt du responsable du traitement ne saurait en aucun cas justifier une exception à l'obligation d'informer de l'art. 24 al. 4 LPD (RAEDLER, *Information*, pp. 121 ss).

¹⁷⁴ CR LPD-MÉTILLE/MEYER, art. 24 N 85 ; RAEDLER, *Information*, p. 123.

¹⁷⁵ Message nLPD, FF 2017 6682.

¹⁷⁶ CR LPD-MÉTILLE/MEYER, art. 24 N 76.

¹⁷⁷ Message nLPD, FF 2017 6682 ; RAEDLER, *Information*, p. 122.

¹⁷⁸ MÉTILLE, *Traitement de données*, p. 17.

¹⁷⁹ CR LPD-RAEDLER, art. 14 N 3.

¹⁸⁰ CR LPD-RAEDLER, art. 14 N 84.

du traitement qui contient les indications mentionnées à l'art. 12 al. 2 LPD, fournir sur demande au PFPDT les indications contenues dans ce registre (art. 15 al. 2 LPD) et fournir sur demande à la personne concernée des renseignements concernant l'exercice de ses droits (art. 15 al. 3 LPD)¹⁸¹.

6. La protection des données dès la conception et protection des données par défaut

La révision de la LPD a introduit l'obligation de mettre en place, dès la conception du traitement, des mesures techniques et organisationnelles afin de garantir le respect des prescriptions en matière de protection des données et en particulier les principes fixés à l'art. 6 LPD (art. 7 al. 1 et 2 LPD). Il ne s'agit pas d'un principe à proprement parler dont la violation constituerait une atteinte à la personnalité au sens de l'art. 30 al. 2 LPD, mais bien plus d'une obligation de prendre de mesures techniques et organisationnelles pour assurer le respect des principes et en particulier celui de la proportionnalité¹⁸².

La protection des données dès la conception repose sur l'idée que la technologie doit être au service de la protection des données personnelles et que la majorité des violations de la sphère privée ne sont pas détectées¹⁸³. Il faut donc éviter qu'elles ne se produisent plutôt que chercher à les sanctionner. La protection technique des données personnelles ne s'appuie pas sur une technologie spécifique, mais elle passe plutôt par la mise en place d'un ensemble de règles techniques et organisationnelles intégrées dans le système, de manière à rendre impossible, ou peu probable, une violation de la protection des données¹⁸⁴.

La protection des données dès la conception matérialise le principe de proportionnalité et l'approche fondée sur les risques¹⁸⁵. Il faut établir un rapport entre le risque induit par le traitement et les moyens techniques permettant de le réduire. Plus le risque est élevé, plus sa survenue est probable, et plus le traitement de données est important, plus les exigences auxquelles doivent répondre les mesures techniques pour être considérées comme appropriées au sens de cette disposition seront élevées¹⁸⁶.

Les mesures techniques et organisationnelles doivent ainsi être appropriées au regard notamment de l'état de la technique, du type de traitement, de son étendue, ainsi que du

¹⁸¹ Cela vise seulement une information générale sur les droits de la personne concernée, par opposition à l'art. 19 LPD qui vise l'accès aux données nécessaires pour qu'elle puisse faire valoir ses droits.

¹⁸² CR LPD-FANTI/STAEGGER, art. 7 N 18.

¹⁸³ Message nLPD, FF 2017 6648.

¹⁸⁴ Message nLPD, FF 2017 6648-6649.

¹⁸⁵ CR LPD-FANTI/STAEGGER, art. 7 N 36.

¹⁸⁶ Message nLPD, FF 2017 6649.

risque que le traitement des données en question présente pour la personne concernée (art. 6 al. 2 LPD)¹⁸⁷.

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

Ainsi sans action spécifique de la personne concernée, elle bénéficie du régime le plus respectueux possible de sa personnalité. Elle ne devrait par exemple pas être obligée de créer un compte client pour effectuer une commande en ligne¹⁸⁸. Ce n'est que si elle choisit de modifier les paramètres prédéfinis qu'elle opte pour une solution différente et consent à un traitement déterminé¹⁸⁹.

VI. Les droits de la personne concernée

A. Les droits déjà connus de l'aLPD

1. Les droits d'opposition et de correction

L'aLPD connaissait déjà les droits de s'opposer au traitement, de faire effacer et détruire des données personnelles, de faire rectifier des données inexacts et d'en faire mentionner le caractère litigieux.

La LPD ne mentionne pas expressément un droit général de s'opposer au traitement de données personnelles, mais cela découle du droit à l'autodétermination informationnelle¹⁹⁰. La LPD mentionne en revanche expressément le droit de s'opposer au traitement dans le cadre d'une action judiciaire (art. 32 al. 2 LPD et 28a CC)¹⁹¹. Rien n'empêche néanmoins de le demander au responsable du traitement en dehors d'une procédure. Le fait, pour un responsable du traitement privé, de traiter (sans motif justificatif) des données personnelles contre la manifestation expresse de la volonté de la

¹⁸⁷ CR LPD-FANTI/STAEGER, art. 7 N 30.

¹⁸⁸ CR LPD-FANTI/STAEGER, art. 7 N 56.

¹⁸⁹ Message nLPD, FF 2017 6649-6650.

¹⁹⁰ Art. 13 Cst., voir notamment : FLÜCKIGER, pp. 846 ss (et les nombreuses références citées à la n. 76).

¹⁹¹ La LPD mentionne également les conséquences d'une opposition, par exemple dans le cas de données rendues accessibles à tout un chacun (art. 17 al. 1 let. e et 30 al. 3 LPD).

personne concernée constitue d'ailleurs une atteinte illicite à la personnalité (art. 30 al. 2 let. b LPD).

La personne concernée peut ainsi toujours s'opposer à un traitement de données la concernant sans avoir à justifier son opposition, son droit étant inconditionnel¹⁹². Cela signifie que la personne concernée n'a pas besoin de le justifier. Il n'est en revanche pas absolu. L'opposition peut intervenir avant ou en cours de traitement et prendre la forme d'une déclaration individuelle ou même une forme plus générale. Elle doit en revanche, et en tout état de cause, être expresse¹⁹³.

Le droit de faire effacer ou détruire des données personnelles est la conséquence du traitement illicite (art. 32 al. 2 let. c LPD). Comme le droit de s'opposer au traitement, de faire rectifier des données inexactes ou d'en faire mentionner le caractère litigieux, le droit de faire effacer et détruire des données est surtout présent dans la LPD comme une prétention à faire valoir dans le cadre d'une procédure judiciaire. Pourtant ces droits correspondent aussi à l'obligation du responsable du traitement de traiter les données dans le respect des principes, en particulier de proportionnalité et d'exactitude.

Le droit de faire effacer ou détruire des données personnelles correspond au « droit à l'oubli », rendu célèbre par la CJUE¹⁹⁴, mais déjà garanti de manière générale par la protection de la personnalité du droit civil¹⁹⁵.

Celui qui traite des données personnelles doit s'assurer qu'elles sont exactes et prendre toutes les mesures appropriées permettant de rectifier, d'effacer ou de détruire les données inexactes ou incomplètes au regard des finalités pour lesquelles elles sont collectées ou traitées (art. 6 al. 5 LPD). Il en découle directement un droit à la rectification, indépendamment de la démonstration d'une atteinte à la personnalité¹⁹⁶. La personne concernée a donc le droit de faire rectifier des données erronées la concernant, sauf si la modification est interdite par une disposition légale (art. 32 al. 1 let. a LPD) ou si les données sont traitées à des fins archivistiques répondant à un intérêt public (art. 32 al. 1 let. b LPD).

Dans le cas particulier où ni l'exactitude ni l'inexactitude d'une donnée personnelle ne peut être établie, la personne concernée peut demander que le responsable du traitement ajoute à la donnée la mention de son caractère litigieux (art. 32 al. 3 LPD). La personne

¹⁹² CR LPD-BOILLAT/WERLY, art. 30 N 26.

¹⁹³ CR LPD-BOILLAT/WERLY, art. 30 N 28.

¹⁹⁴ Message nLPD, FF 2017 6693 ; CJUE, C-131/12, ECLI:EU:C:2014:317, (*Google Spain SL, Google Inc. Contre Agencia Española de Protección de Datos (AEPD) et Mario Costeja González*).

¹⁹⁵ CR LPD-BOILLAT/WERLY, art. 32 N 26.

¹⁹⁶ Message nLPD, FF 2017 6693. Voir également : CR LPD-BOILLAT/WERLY, art. 32 N 10. Avis contraire : ROSENTHAL, nDSG, N 139.

concernée peut aussi obtenir que l'effacement ou la destruction des données personnelles, leur rectification ou la mention du caractère litigieux soit communiquée à des tiers (notamment les destinataires) ou publiée (art. 32 al. 4 LPD).

2. Le droit d'accès

Si comme nous l'avons vu le droit d'être informé spontanément a été renforcé par l'obligation d'informer du responsable du traitement (alors que l'aLPD se contentait dans la plupart des cas d'une simple reconnaissabilité), le droit d'accès (qui recouvre d'une part le droit d'être informé sur demande et d'autre par le droit de consulter ses données) reste relativement inchangé (art. 25 ss LPD)¹⁹⁷.

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 loi¹⁹⁸. C'est un droit subjectif inhérent à la personne, que même une personne qui n'a pas l'exercice des droits civils mais qui est capable de discernement peut faire valoir seule et sans avoir à requérir le consentement de son représentant légal, et auquel il ne peut pas être renoncé valablement par avance¹⁹⁹.

Le droit d'accès consacre premièrement pour toute personne le droit de savoir si des données personnelles la concernant sont traitées (art. 25 al. 1 LPD). Il consacre deuxièmement le droit d'en recevoir une copie (art. 25 al. 2 let. b LPD) et troisièmement celui de recevoir des informations sur l'identité et les coordonnées du responsable du traitement (art. 25 al. 2 let. a LPD), la finalité du traitement (art. 25 al. 2 let. c LPD), la durée de conservation ou au moins les critères pour la fixer (art. 25 al. 2 let. d LPD), les éventuels destinataires ou catégories de destinataires auxquels des données personnelles sont communiquées (art. 25 al. 2 let. g LPD), les informations disponibles sur l'origine des données si elles n'ont pas été collectées auprès de la personne concernée (art. 25 al. 2 let. e LPD), l'existence éventuelle d'une décision individuelle automatisée ainsi que la logique sur laquelle se base cette décision (art. 25 al. 2 let. f LPD), la liste des Etats étrangers vers lesquels les données sont exportées (y compris les garanties appropriées ou les motifs d'exception)²⁰⁰, et finalement toute autre information nécessaire pour que la personne

¹⁹⁷ Sur le droit d'accès en général, voir : HERTIG PEA, N 109 ss ; BENHAMOU, pp. 77 ss ; D'ERRICO LUCA, pp. 107 ss ; ROUILLER/EPINEY, pp. 1 ss ; PÄRLI/EGGMANN, pp. 140 ss ; GRIESINGER MARCEL.

¹⁹⁸ CR LPD-BENHAMOU, art. 25 N 8.

¹⁹⁹ Message nLPD, FF 2017 6682.

²⁰⁰ L'art. 25 al. 2 let. g LPD prévoit d'une part que le responsable du traitement doit indiquer les destinataires ou les catégories de destinataires auxquels des données personnelles sont communiquées et, d'autre part, les informations prévues à l'art. 19 al. 4 LPD. C'est ainsi que la liste des Etats étrangers doit être communiquée à la personne exerçant sa demande de droit d'accès. Conformément à l'art. 19

concernée puisse faire valoir ses droits selon la LPD et pour que la transparence du traitement soit garantie (art. 25 al. 2 LPD)²⁰¹.

La demande et la réponse se font par écrit, y compris en la forme électronique²⁰². Avec l'accord du responsable du traitement, la demande peut se faire oralement et la consultation sur place (art. 16 OPDo). En principe, le responsable du traitement doit répondre dans les 30 jours (art. 18 OPDo) et gratuitement (art. 19 OPDo)²⁰³. Lorsqu'il s'agit de données liées à la santé, il peut les communiquer à la personne concernée par l'intermédiaire d'un professionnel de la santé qu'elle aura désigné, si elle est d'accord avec cette manière de procéder²⁰⁴.

Si le droit d'accès est inconditionnel et ne demande pas de justification, il n'est pas absolu. Dans certains cas, le responsable du traitement peut refuser, restreindre ou différer la communication de renseignements. Il doit néanmoins indiquer à la personne concernée qu'il refuse, restreint ou diffère la communication des informations et le motif invoqué (art. 26 al. 4 LPD).

Plusieurs motifs peuvent être invoqués par un responsable du traitement privé. Premièrement, une loi formelle peut prévoir que les informations ne doivent pas être communiquées, par exemple pour protéger le secret professionnel (art. 26 al. 1 let. a LPD). Deuxièmement, la protection des intérêts de tiers, notamment la protection de leur sphère privée, peut s'opposer à la communication (art. 26 al. 1 let. b LPD). Troisièmement et seulement si les données ne sont pas transmises à un tiers, le responsable du traitement privé peut faire valoir son propre intérêt prépondérant (art. 26 al. 2 let. a LPD). Cet intérêt doit être suffisamment important pour être considéré comme prépondérant²⁰⁵. Quatrièmement, les médias et journalistes bénéficient de règles particulières pour assurer la liberté de la presse (art. 27 LPD). Cinquièmement, le responsable du traitement peut encore invoquer le principe de l'abus de droit (art. 2 al. 2 CC)²⁰⁶ et le caractère manifestement infondé de la demande, notamment parce qu'elle poursuit un but contraire

al. 4 LPD, et cas échéant, le responsable du traitement doit communiquer les garanties prévues à l'art. 16 al. 2 LPD ou les motifs d'exception prévus à l'art. 17 LPD.

²⁰¹ CR LPD-BENHAMOU, art. 25 N 8.

²⁰² CR LPD-BENHAMOU, art. 25 N 57.

²⁰³ Une participation adéquate (mais limitée à CHF 300.-) peut être demandée à la personne concernée si la communication des renseignements occasionne des efforts disproportionnés. La personne concernée doit néanmoins en être informée préalablement. Elle doit confirmer sa demande dans un délai de 10 jours, sans quoi elle est considérée comme retirée sans frais (art. 19 OPDo).

²⁰⁴ L'aLPD permettait, de manière très discutable, de l'imposer à la personne concernée. La LPD impose désormais à raison le consentement de la personne concernée pour cette remise indirecte. MEIER, Précis, N 1006 ; Message nLPD, FF 2017 6684.

²⁰⁵ Par exemple pour protéger ses secrets d'affaires (CR LPD-BENHAMOU, art. 26 N 19).

²⁰⁶ Sur le caractère abusif du droit d'accès, voir : ROUILLER/EPINEY, pp. 13 ss.

à la protection des données ou qu'elle est manifestement procédurière (art. 26 al. 1 let. c LPD). C'est le cas d'une demande répétée sans raison, mais pas d'une simple marque de curiosité. Le Tribunal fédéral a eu l'occasion de préciser qu'une demande de droit d'accès qui visait à se procurer des preuves en vue d'une procédure civile sans chercher à vérifier les données ou le traitement effectué était abusive.²⁰⁷.

B. Les nouveaux droits

1. En matière d'information

Le droit de la personne concernée à être informée spontanément du traitement de ses données personnelles est garanti par le principe de transparence et surtout l'obligation d'information (art. 19 LPD)²⁰⁸. Quant au droit d'être informé en cas de violation de la sécurité des données, il est prévu par l'obligation correspondante du responsable du traitement (art. 24 LPD)²⁰⁹.

2. En matière de décision individuelle automatisée

L'art. 21 LPD introduit des droits spécifiques en cas de décision individuelle automatisée qui a des effets juridiques sur la personne concernée ou qui l'affecte de manière significative : un droit d'information, un droit pour la personne concernée de faire valoir son point de vue sur le résultat de la décision, un droit de connaître comment la décision a été prise et un droit de faire revoir la décision automatisée par une personne physique²¹⁰. Le but est notamment d'éviter que le traitement de données soit effectué sur la base de données incomplètes, dépassées ou non pertinentes, ou plus généralement de manière discriminatoire²¹¹.

Par décision individuelle automatisée, il faut entendre une décision prise exclusivement sur la base d'un traitement de données personnelles automatisé sans qu'une décision ne soit prise par une personne physique sur la base de sa propre évaluation de la situation. Les décisions simples du genre de celles qui sont prises lors d'un retrait au bancomat

²⁰⁷ TF 4A_277/2020 du 18 novembre 2020. Contrairement aux ATF 138 III 425 et ATF 141 III 119 où l'intérêt des requérants à vérifier les données, respectivement le traitement, enlevait le caractère abusif du droit d'accès (même s'il ne faisait pas de doute qu'il s'agissait aussi d'une volonté de réunir des preuves).

²⁰⁸ Cf. *supra* V.B.3.

²⁰⁹ Cf. *supra* V.B.4.

²¹⁰ RAEDLER, *Information*, pp. 113 ss.

²¹¹ Sur la décision individuelle automatisée dans le cadre du travail, voir : CÉLIAN HIRSCH, pp. 97 ss du présent ouvrage.

(délivrance du montant demandé si le solde en compte est suffisant) ne sont pas concernées²¹². Le fait que la décision soit communiquée par une personne physique ne change rien à son caractère automatisé, car cette personne n'a pas d'influence sur le processus de décision et son résultat²¹³.

Ces obligations ne s'appliquent que si la décision a des effets juridiques pour la personne concernée²¹⁴ ou l'affecte de manière significative²¹⁵. En revanche, ces obligations ne s'appliquent pas lorsque la décision est en relation directe avec la conclusion ou l'exécution d'un contrat entre le responsable du traitement et la personne concernée et que la demande de cette dernière est satisfaite (art. 21 al. 3 let. a LPD), ou encore si la personne concernée a expressément consenti à ce que la décision soit prise de manière automatisée (art. 21 al. 3 let. b LPD). Dans le premier cas, on suppose que l'information n'intéresse plus la personne concernée, alors que dans le second elle a déjà reçu l'information avant de donner un consentement juridiquement valable²¹⁶.

3. Le droit à la remise ou à la transmission des données

L'Assemblée fédérale a introduit le droit à la remise ou à la transmission des données personnelles (art. 28 LPD), plus connu sous la notion de droit à la portabilité²¹⁷. Ce droit permet à la personne concernée d'obtenir gratuitement les données qu'elle a fournies, voire de les faire remettre directement à un autre responsable du traitement. Il vise à défendre l'autonomie de la personne concernée vis-à-vis d'un responsable du traitement, ce qui est un aspect de la protection de la personnalité, mais surtout une incitation à encourager la concurrence et l'arrivée de nouveaux fournisseurs de services sur le marché²¹⁸.

Par données fournies, il faut comprendre toutes les données que la personne concernée a mises délibérément et en connaissance de cause à disposition du responsable du traitement, mais également toutes les données que le responsable du traitement a collectées au sujet de la personne concernée et qui concernent son comportement dans le cadre de l'utilisation d'un service ou d'un appareil²¹⁹. En revanche, les données personnelles que le responsable

²¹² CR LPD-FLUECKIGER, art. 21 N 4 ; RAEDLER, Information, p. 113.

²¹³ Message nLPD, FF 2017 6674.

²¹⁴ Par exemple, la conclusion ou la dénonciation d'un contrat (ROSENTHAL, nDSG, N 109).

²¹⁵ Par exemple, la personne concernée est entravée sur le plan économique ou personnel. Il est nécessaire de prendre en compte l'importance du bien en question, la durée des effets de la décision et l'existence ou non d'une solution de remplacement (Message nLPD, FF 2017 6674).

²¹⁶ CR LPD-FLUECKIGER, art. 21 N 12 ; Message nLPD, FF 2017 6675 ; RAEDLER, Information, p. 117.

²¹⁷ CR LPD-BENHAMOU, art. 28 N 1 ; GÖTZINGER/VASELLA, p. 40.

²¹⁸ CR LPD-BENHAMOU, art. 28 N 4 ; GÖTZINGER/VASELLA, p. 41.

²¹⁹ CR LPD-BENHAMOU, art. 28 N 21.

du traitement a générées en évaluant les données personnelles fournies ne sont pas soumises au droit à la remise ou à la transmission (art. 20 OPDo)²²⁰.

Les données doivent être remises dans un format électronique courant, soit un format qui permet de réutiliser les données sans effort disproportionné (art. 21 OPDo). Un format « courant » devrait tenir compte de la branche concernée, du type de données en question et de la zone géographique pertinente²²¹.

Ce droit ne s'applique que si les données sont traitées de manière automatisée et que ce traitement, soit repose sur le consentement de la personne concernée, soit est en relation directe avec la conclusion ou l'exécution d'un contrat entre elle et le responsable du traitement²²². Cette condition du consentement ou de la nécessité contractuelle est étrangère au droit suisse et malheureuse. Il ne s'agit pas de conditions justifiant un traitement (comme cela est prévu dans l'Union européenne par le Règlement général sur la protection des données de données) et permettant d'identifier certaines catégories de traitement, mais de motifs justifiant une atteinte à la personnalité. Ainsi, le droit à la portabilité, dont on rappelle qu'il doit faciliter le passage à un autre responsable du traitement, n'existerait qu'en cas d'atteinte à la personnalité. Il ne fait guère de doute que cela n'était pas l'intention de l'Assemblée fédérale. Le PFPDT et les tribunaux devront donc interpréter cette disposition selon son but et non selon sa lettre, et ne pas limiter le droit à la portabilité aux cas d'atteinte à la personnalité.

VII. La procédure et la surveillance

Les procédures judiciaires et la procédure devant le PFPDT étant traitées dans cet ouvrage par DAVID RAEDLER, il y est renvoyé²²³. On se contentera de mentionner brièvement les nouveautés par rapport à l'aLPD.

S'agissant des moyens d'action devant la justice civile, on pense surtout aux actions en cas d'atteinte à la personnalité des art. 28 ss CC et 32 LPD, mais la personne concernée peut aussi saisir la justice si on lui refuse un droit d'accès ou à la remise de ses données personnelles. Elle peut également faire valoir des moyens réparateurs tels que des

²²⁰ GÖTZINGER/VASELLA, p. 42.

²²¹ GÖTZINGER/VASELLA, pp. 48 ss.

²²² CR LPD-BENHAMOU, art. 28 N 29.

²²³ RAEDLER, pp. 153 ss du présent ouvrage. Voir également CR LPD-BOILLAT/WERLY, art. 32 ; MÉTILLE, Nouvelle loi, pp. 23 ss.

prétentions en réparation du dommage subi (art. 41 et 97 CO), y compris le tort moral (art. 49 CO), voire en remise de gain (art. 421 al. 1 CO).

La principale modification concerne la suppression des frais de justice pour les actions civiles relevant de la protection des données. Le but est de simplifier la mise en œuvre procédurale des droits des personnes concernées, et d'augmenter l'efficacité de la LPD en évitant que les personnes concernées renoncent à faire valoir leurs droits en raison notamment du risque de devoir supporter les coûts de procédure²²⁴.

Ainsi, il n'est plus perçu de frais judiciaires pour la procédure de conciliation (art. 113 al. 2 let. g CPC) et pour la procédure au fond (art. 114 let. g CPC) dans les litiges relevant de la LPD, et cela indépendamment de la valeur litigieuse. Le demandeur est également dispensé de fournir des sûretés (art. 99 al. 3 lit. d CPC).

En revanche, les dépens continuent d'être répartis selon les normes usuelles (art. 104 ss CPC) et le demandeur doit assumer ses propres frais de représentation. Comme il n'est en principe pas accordé de dépens en procédure de conciliation (art. 113 al. 1 CPC), le risque est donc limité au moins dans cette première phase. A noter encore que ces nouvelles règles de procédure s'appliquent depuis le 1^{er} septembre 2023, qu'il s'agisse de procédures nouvelles ou pendantes (art. 407e CPC).

Au niveau pénal, la LPD fixe une série de dispositions pénales remaniées aux art. 60 ss afin de renforcer le dispositif répressif en matière de protection des données personnelles²²⁵.

Les contraventions pénales de la LPD concernent d'abord la violation des obligations d'informer et de renseigner (art. 60 al. 1 LPD) par exemple en fournissant des renseignements inexacts ou incomplets en violation du devoir général d'informer lors de la collecte de données personnelles (art. 19 LPD), en l'absence d'exceptions (art. 20 LPD), en violation du devoir d'informer en cas de décision individuelle automatisée (art. 21 LPD) ou en violation du droit d'accès (art. 25 LPD), en l'absence de restrictions (art. 26 ss LPD), ou encore en ne fournissant aucune information en violation des devoirs d'informer précités. *A contrario*, l'absence complète de réponse à une demande de droit d'accès ou de remise de données n'est pas une infraction pénale²²⁶.

Elles concernent ensuite la violation des devoirs de diligence en cas de sous-traitance, de transfert à l'étranger et en matière de sécurité (art. 61 LPD) par exemple dans l'hypothèse d'une communication des données dans un pays inadéquat sans garanties ou dérogations

²²⁴ Message nLPD, FF 2017 6637 ss.

²²⁵ Concernant les dispositions pénales de la LPD, nous renvoyons de manière générale à : CR LPD-MÉTILLE, art. 60 ss ; Message nLPD, FF 2017 6714 ; JACOT-GUILLARMOD/THORENS, pp. 11 ss ; PAHUD/PITTET ; ROSENTHAL/GUBLER.

²²⁶ CR LPD-MÉTILLE, art. 60 N 9.

(art. 16 ss LPD), du recours à un sous-traitant sans respecter les exigences en la matière (art. 9 LPD), ou d'une violation des exigences minimales de sécurité selon l'OPDo (art. 8 al. 3 LPD).

Elles concernent finalement la violation de collaborer avec le PFPDT (art. 60 al. 2 LPD), notamment en fournissant des renseignements inexacts au PFPDT ou en refusant de collaborer dans le cadre d'une enquête (art. 49 al. 3 LPD), en l'absence d'un droit de refuser de témoigner (art. 16 ss PA), et l'insoumission à une décision du PFPDT ou d'une autorité de recours, alors que la décision a été signifiée sous menace de la peine prévue à l'art. 63 LPD²²⁷. On peut encore mentionner brièvement la violation du devoir de discrétion (art. 62 LPD) et l'usurpation d'identité (art. 179^{decies} CP).

On relèvera que toutes les infractions sont intentionnelles ; la négligence n'est pas punie. L'action pénale se prescrit par cinq ans (art. 66 LPD)²²⁸ et les autorités pénales cantonales de poursuite sont compétentes (art. 65 al. 1 LPD). Le PFPDT peut toutefois dénoncer des infractions et faire valoir les droits d'une partie plaignante (art. 60 al. 2 LPD).

En outre, l'art. 64 LPD fait application des dispositions des art. 6 et 7 DPA s'agissant des infractions commises dans une entreprise afin de rendre possible, sous certaines conditions, la poursuite des chefs d'entreprise, employeur, mandant ou représenté ainsi que les entreprises elles-mêmes lorsque l'amende entrant en ligne de compte ne dépasse pas CHF 50'000.-et que l'enquête rendrait nécessaires à l'égard des personnes physiques punissables des mesures d'instruction hors de proportion avec la peine encourue (art. 64 al. 2 LPD).

Quant à la procédure administrative devant le PFPDT²²⁹, la principale nouveauté est que la personne concernée peut désormais saisir le PFPDT, qui est tenu d'ouvrir une enquête d'office ou sur dénonciation dès que des indices font penser que des traitements de données pourraient être contraires à des dispositions légales de protection des données (art. 49 al. 1 LPD). Le dénonciateur, même si c'est la personne concernée, n'a pas qualité de partie à la procédure (art. 52 al. 2 LPD *a contrario*)²³⁰. Il sera toutefois informé de la suite donnée à sa dénonciation et du résultat de l'éventuelle enquête (art. 49 al. 4 LPD).

A l'issue de son enquête, le PFPDT peut prononcer des mesures administratives contraignantes (art. 51 LPD). Le responsable du traitement et le sous-traitant visé peuvent évidemment recourir contre la décision du PFPDT. Ce dernier dispose également de la

²²⁷ Lorsque la décision du PFPDT s'adresse à une entreprise, c'est une personne physique occupant une fonction dirigeante qui sera punissable (art. 29 CP ; Message nLPD, FF 2017 6718).

²²⁸ La prescription de l'action pénale pour les contraventions est normalement de trois ans (art. 109 CP).

²²⁹ Concernant la procédure administrative de la LPD, nous renvoyons de manière générale à : CR LPD-RAEDLER, art. 52 ; PFPDT, Application des art. 49 à 53 LPD, pp. 1 ss.

²³⁰ Message nLPD, FF 2017 6708.

qualité pour recourir cas échéant contre les décisions sur recours du Tribunal administratif fédéral (art. 52 al. 3 LPD).

Le PFPDT peut également dénoncer les infractions à la LPD dont il a connaissance aux autorités pénales compétentes et faire valoir les droits d'une partie plaignante dans le cadre de la procédure pénale (art. 65 al. 2 LPD).

Les mesures que le PFPDT peut prendre qui concernent tous les traitements de données contraires à des dispositions de protection des données. Cela va du simple avertissement à l'ordre de cesser le traitement ou de détruire des données personnelles (art. 51 al. 1 et 5 LPD). Le PFPDT peut aussi interdire la communication de données personnelles à l'étranger (art. 51 al. 2 LPD). Des mesures peuvent finalement être prises en cas de non-observation de prescriptions d'ordre ou des devoirs à l'égard de la personne concernée (art. 51 al. 3 et 4 LPD). Le PFPDT peut, par exemple, ordonner au responsable du traitement de prendre des mesures techniques et organisationnelles (art. 51 al. 3 let. b LPD), d'établir une analyse d'impact (art. 51 al. 3 let. d LPD) et de le consulter (art. 51 al. 3 let. e LPD), d'annoncer une violation de la sécurité (art. 51 al. 3 let. f LPD), de communiquer les informations requises en matière de transfert à l'étranger (art. 51 al. 3 let. a LPD) ou de désigner un représentant (art. 51 al. 4 LPD)²³¹.

VIII. Conclusion

La LPD est le fruit d'une révision totale, du moins c'est ainsi qu'elle a été qualifiée. Sur le papier, les nouveautés sont nombreuses : renforcement de droits et d'obligations, introduction de la possibilité pour le PFPDT de rendre des décisions contraignantes, renforcement des sanctions pénales, gratuité des procédures civiles, etc. Dans les faits, les moyens du PFPDT n'ont été que légèrement renforcés et les autorités de poursuite pénale en matière de contravention ne sont évidemment guère armées pour juger des questions de protection des données.

La LPD est ainsi fort utile pour celui qui veut la respecter et souhaite savoir quelle est la ligne à ne pas dépasser, même si on peut discuter de l'utilité pour un responsable du traitement de consacrer de l'énergie à certaines formalités (registre, AIPD, etc.) plutôt que de se concentrer sur l'essentiel comme le respect des principes ou la protection des données dès la conception et par défaut. La LPD reste en revanche peu impressionnante pour celui qui a un intérêt (financier, matériel, personnel, etc.) à la violer. La personne concernée devra malheureusement encore beaucoup compter sur elle-même pour défendre sa

²³¹ CR LPD-RAEDLER, art. 51 N 39 ss.

personnalité atteinte par un traitement illicite de données et engager une procédure judiciaire contre le responsable du traitement, avec toutes les difficultés que l'on connaît.

Bibliographie

- BAERISWYL BRUNO/PÄRLI KURT/BLONSKI DOMINIKA (édit.), *Stämpfli's Hankommentar Datenschutzgesetz (DSG)*, 2^e éd., Berne 2023 (cité : SHK DSG-AUTEUR, art. ... N ...).
- BENHAMOU YANIV, *Mise en œuvre judiciaire du droit d'accès LPD – aspects procéduraux choisis*, in : Métille (édit.), *Le droit d'accès*, Berne 2021, pp. 77 ss.
- BENHAMOU YANIV/COTTIER BERTIL (édit.), *Loi fédérale sur la protection des données*, Petit Commentaire, Bâle 2023 (cité : PC LPD-AUTEUR, art. ... N ...).
- COMITÉ EUROPÉEN DE LA PROTECTION DES DONNÉES, *Recommandation 01/2019 sur le projet de liste établi par le Contrôleur européen de la protection des données concernant les opérations de traitement pour lesquelles une analyse d'impact relative à la protection des données est requise* (art. 39 par. 4 du règlement (UE) 2018/1725) du 10 juillet 2019 (disponible en ligne : https://edpb.europa.eu/our-work-tools/our-documents/recommendations/recommendation-012019-draft-list-european-data_fr [consulté le 21.03.2024]).
- CONSEIL FÉDÉRAL, *Message du 15 septembre 2017 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 FF 2017 6565* (cité : Message nLPD).
- D'ERRICO LUCA, *Répondre à une demande de droit d'accès – aspects pratiques*, in : Métille (édit.), *Le droit d'accès*, Berne 2021, pp. 107 ss.
- EPINEY ASTRID/NÜESCH DANIELA/ROVELLI SOPHIA, *Datenschutzrecht in der Schweiz – Eine Einführung in das Datenschutzgesetz des Bundes, mit besonderem Akzent auf den für Bundesorgane relevanten Vorgaben*, Berne 2023.
- FLÜCKIGER ALEXANDRE, *L'autodétermination en matière de données personnelles : un droit (plus si) fondamental à l'ère digitale ou un nouveau droit de propriété ?*, PJA 2013, vol. 22, n° 6, pp. 837 ss.
- GILLIÉRON PHILIPPE, *Conseiller à la protection des données, registre des activités de traitement et analyse d'impact*, in : Bernasconi/Passucci (édit.), *Protezione dei dati personali : orizzonte 2023 – Introduzione alle nuove norme di livello federale e cantonale*, Lugano 2023, pp. 81 ss (cité : GILLIÉRON, Conseiller, registre et analyse).
- GÖTZINGER LENA/VASELLA DAVID, *Datenportabilität und ihre Umsetzung*, RSDA 1/2021, pp. 40 ss.
- GRIESINGER MARCEL, *Der datenschutzrechtliche Auskunftsanspruch nach Art. 15 DSGVO*, in : Jusletter du 20 janvier 2020.
- GROUPE DE TRAVAIL « ARTICLE 29 » SUR LA PROTECTION DES DONNÉES, *Lignes directrices concernant l'analyse d'impact relative à la protection des données (AIPD) et la manière de déterminer si le traitement est « susceptible d'engendrer un risque élevé » aux fins du règlement (UE) 2016/679 du 4 octobre 2017* (disponible en ligne à : <https://ec.europa.eu/newsroom/article29/items/611236/en> [consulté le 21.03.2024]).
- HERTIG PEA AGNÈS, *La protection des données personnelles médicales est-elle efficace ? – Etude des moyens d'action en droit suisse*, thèse Neuchâtel, Bâle 2013.
- JACOT-GUILLARMOD ÉMILIE, *Le profilage à risque élevé de la LPD : réflexions autour d'un monstre de Frankenstein*, in : Swissprivacy.law 24 août 2021.
- JACOT-GUILLARMOD ÉMILIE/THORENS OLAF, *Les nouveaux pouvoirs du PFPDT et son rôle dans la poursuite pénale en vertu de la LPD*, in : Jusletter 25 septembre 2023.

- MAURER-LAMBROU URS/BLECHTA GABOR P. (édit.), *Datenschutzgesetz (DSG)/Öffentlichkeitsgesetz (BGÖ)*, Basler Kommentar, 3^e éd., Bâle 2014 (cité : BSK DSG-AUTEUR, art. ... N ...).
- MEIER PHILIPPE, *Droit des personnes – Personnes physiques et morales*, art. 11-89a CC, 2^e éd., Zurich 2021.
- MEIER PHILIPPE, *Protection des données – Fondements, principes généraux et droit privé*, Berne 2010 (cité : MEIER, Précis).
- MEIER PHILIPPE/MÉTILLE SYLVAIN, *Loi fédérale sur la protection des données*, Commentaire romand, Bâle 2023 (cité : CR LPD-AUTEUR, art. ... N ...)
- MÉTILLE SYLVAIN, *La (nouvelle) Loi fédérale sur la protection des données du 25 septembre 2020 : des principes, des droits et des obligations*, in : Epiney/Moser/Rovelli (édit.), *Die Revision des Datenschutzgesetzes des Bundes/La révision de la Loi fédérale sur la protection des données*, Zurich 2022, pp. 1 ss (cité : MÉTILLE, Nouvelle loi).
- MÉTILLE SYLVAIN, *Le traitement de données personnelles sous l'angle de la (nouvelle) Loi fédérale sur la protection des données du 25 septembre 2020*, SJ 2021 II, pp. 1 ss (cité : MÉTILLE, Traitement de données).
- MÉTILLE SYLVAIN/ACKERMANN ANNELEISE, *RGPD : application territoriale et extraterritoriale*, in : Epiney/Rovelli (édit.), *Datenschutzgrundverordnung (DSGVO) : Tragweite und erste Erfahrungen/Le règlement général sur la protection des données (RGPD) : portée et premières expériences*, Zurich 2020, pp. 77 ss.
- MÉTILLE SYLVAIN/ARASTEH YASMINE, *Le Règlement général sur la protection des données et les assureurs privés suisses*, in : Fuhrer (édit.), *Annales SDRCA 2018*, Zurich/Bâle/Genève 2018, pp. 107 ss.
- MÉTILLE SYLVAIN/NGUYEN XUAN NADJA, *Un profil de personnalité n'est pas nécessaire pour juger de la solvabilité d'une personne*, Medialex 2017, pp. 176 ss.
- PAHUD JOËL/PITTET SÉBASTIEN, *Les infractions pénales de la loi sur la protection des données*, in : Jusletter du 25 septembre 2023.
- PÄRLI KURT/EGGMANN JONAS, *Das Auskunftsrechts im Privatrecht*, digma 3/2020, pp. 140 ss.
- PRÉPOSÉ FÉDÉRAL À LA PROTECTION DES DONNÉES ET À LA TRANSPARENCE, *Enquêtes du PFPDT concernant des violations des prescriptions de protection des données – Application des art. 49 à 53 de la loi sur la protection des données révisée*, Berne 2023 (cité : PFPDT, Application des art. 49 à 53 LPD).
- PRÉPOSÉ FÉDÉRAL À LA PROTECTION DES DONNÉES ET À LA TRANSPARENCE, *Aide-mémoire concernant l'analyse d'impact relative à la protection des données personnelles (AIPD) au sens des art. 22 et 23 LPD*, Berne 2023 (cité : PFPDT, Aide-mémoire).
- PRÉPOSÉ FÉDÉRAL À LA PROTECTION DES DONNÉES ET À LA TRANSPARENCE, *Transfert de données personnelles dans un pays ne présentant pas le niveau de protection des données requis, en application de clauses contractuelles types et de contrats types reconnus* 27 août 2021, Berne 2021 (cité : PFPDT, Transfert de données personnelles).
- RAEDLER DAVID, *L'information en droit de la protection des données, entre obligations, exceptions et sanction*, in : Bernasconi/Passucci (édit.), *Protezione dei dati personali : orizzonte 2023 – Introduzione alle nuove norme di livello federale e cantonale*, Lugano 2023, pp. 81 ss (cité : RAEDLER, Information).

- ROSENTHAL DAVID, Controller oder Processor : Die datenschutzrechtliche Gretchenfrage, *in* : Jusletter du 17 juin 2019 (cité : ROSENTHAL, Controller oder Processor).
- ROSENTHAL DAVID, Das neue Datenschutzgesetz, *in* : Jusletter du 16 novembre 2020 (cité : ROSENTHAL, nDSG).
- ROSENTHAL DAVID/GUBLER SERAINA, Die Strafbestimmungen des neuen DSG, RSDA 1/2021, pp. 52 ss.
- ROUILLER FÉLISE/EPINEY ASTRID, Le droit d'accès à ses données personnelles, *in* : Métille (édit.), Le droit d'accès, Berne 2021, pp. 1 ss.
- THOUVENIN FLORENT *et al.*, Privacy Icons : Transparenz auf einen Blick, *in* : Jusletter du 30 novembre 2020.