La nouvelle loi suisse de protection des données dans le contexte international (Convention 108+ et RGPD)

De Terwangne, Cecile

Published in:
Die Revision des Datenschutzgesetzes des Bundes - La révision de la Loi fédérale sur la protection des données,

Publication date:
2022

Document Version
le PDF de l'éditeur

La nouvelle loi suisse de protection des données dans le contexte international (Convention 108+ et RGPD)

Cécile de Terwangne

Sommaire

A. Introduction

La loi suisse de protection des données aura vécu trente ans dans sa mouture du vingtième siècle avant d'être fondamentalement révisée pour être en phase avec la réalité et les défis du vingt-et-unième siècle. Datant du 25 juin 1992, la loi dans sa première version n'avait pas pu anticiper le déploiement d'Internet, l'apparition des objets intelligents et connectés (les *smartphones, smart TV, smart watches, smart cars,…*), des lieux intelligents et tout aussi connectés (les *smart houses, smart schools, smart cities*,…) et la montée en puissance du *Big data* et de l'intelligence artificielle. *Yahoo* et *Amazon* (fondées en 1994), *Google* (en 1998), *Facebook* (en 2004) et *Twitter* (en 2006) n'avaient pas encore façonné le monde comme ils allaient peu à peu le faire. Même si elles accompagnaient et alimentaient déjà la plupart des activités humaines, les données personnelles n'étaient pas encore devenues un trésor de guerre suscitant la convoitise des acteurs économiques et générant des milliards de dollars de bénéfice.

La radicalité du changement de société dans les trente dernières années a conduit à la nécessité de revoir les textes juridiques garantissant la protection des données à caractère personnel. Parmi ces textes, deux textes européens ont exercé une influence décisive sur les législations adoptées par les Etats du continent : la Convention 108 du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel[1] et la directive 95/46/CE de l'Union européenne.[2]

La Convention 108 a fait l'objet d'une opération de modernisation ayant abouti à l'adoption d'un Protocole d'amendement le 18 mai 2018.[3] Le résultat de cette modernisation est appelé la Convention 108+. Le Protocole d'amendement a été ouvert à signature le 10 octobre 2018 et a recueilli jusqu'à présent[4] quarante-trois signatures. La Suisse a signé le Protocole le 21 novembre 2019. A ce jour, quinze Etats ont procédé à sa ratification. Il faudra compter trente-huit Parties au plus tard à la date du 11 octobre 2023 pour que le Protocole entre en vigueur. Dans l'hypothèse où ce ne serait pas le cas, le Protocole n'entrera alors en vigueur que lorsqu'il

1 Convention 108 du 28 janvier 1981.

2 Directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, L 281/31.

3 Protocole d'amendement à la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (STCE n° 223), adopté par le Comité des Ministres du CoE le 18 mai 2018 à Elseneur, ouvert à signature le 10 octobre 2018.

4 Novembre 2021.

sera ratifié par toutes les Parties à la Convention 108. La Convention 108+, en tant que traité international, est le seul texte juridiquement contraignant de portée internationale en matière de protection des données.

Quant à la directive 95/46, elle a cédé la place au très médiatique règlement général sur la protection des données[5] (RGPD ou, en anglais, *GDPR*), adopté le 27 avril 2016 par l'Union européenne et entré en application depuis le 25 mai 2018. Ce texte ne fait pas partie de l'acquis de Schengen. La Suisse n'est donc pas tenue de le reprendre en vertu de l'accord d'association à Schengen.[6] Par contre, de par les critères définissant son champ d'application territorial (cf. *infra* C.), le RGPD a vocation à s'appliquer dans bien des cas au-delà des frontières de l'Union européenne. Nombreux sont les acteurs économiques suisses devant tenir compte de ce texte dans le cadre de leurs activités depuis mai 2018.[7]

Les pages qui suivent présentent conjointement la Convention 108+ et le RGPD, similaires sur de nombreux points. Leurs spécificités sont clairement indiquées. Pour chacun des aspects évoqués, la présentation du contenu équivalent de la nouvelle loi fédérale du 25 septembre 2020 sur la protection des données (ci-après LPD) permet de mettre en exergue et d'analyser les similitudes et divergences de la loi suisse au regard des deux textes européens.

5 Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données), L 119/1 (en anglais : *general data protection regulation*, *GDPR*).

6 Contrairement à la directive (UE) 2016/680 adoptée le même jour par l'UE, que la Suisse doit reprendre au titre de l'acquis de Schengen ; cf. Message concernant la loi fédérale sur la révision totale de la loi fédérale sur la protection des données et sur la modification d'autres lois fédérales, FF 2017 6565, 6587.

7 Préposé fédéral à la protection des données et à la transparence (ci-après PFPDT), The new Data Protection Act from the FDPIC's perspective, 9 février 2021, <https://www.edoeb.admin.ch/edoeb/en/home/latest-news/aktuell_news.html#-2053438021>, 3: « When revising the FADP, the Federal Council and Parliament took account of the protocol amending the Convention of the Council of Europe 1081 that has been signed by Switzerland, and the General Data Protection Regulation of the European Union (GDPR). Owing to its extraterritorial scope, the latter has already been applied by large parts of the Swiss economy since it entered into force in May 2018. ; cf. égal. *Cornelia Stengel*/*Luca Stäuble*, Protection des données: tour d'horizon de la nouvelle loi, 19 mai 2021, economiesuisse, <https://www.economiesuisse.ch/fr/articles/protection-des-donnees-tour-dhorizon-de-la-nouvelle-loi>.

B. Proclamation du droit à la protection des données à caractère personnel en lien avec les droits fondamentaux et la dignité humaine

Tant la Convention 108+ que le RGPD proclament le droit de toute personne à la protection de ses données à caractère personnel.[8] Selon le Préambule de la Convention 108+, il s'agit du « droit de la personne de contrôler ses propres données à caractère personnel et le traitement qui en est fait ». Garantir aux individus le droit à la protection de leurs données vise à les mettre en position de connaître, de comprendre et de contrôler le traitement de leurs données à caractère personnel opéré par des tiers.

La réalité concernant le sort des données à caractère personnel dans l'environnement numérique d'aujourd'hui échappe dans bien des cas aux intéressés : données recueillies à l'insu des personnes, données réutilisées pour des finalités inavouées, données conservées des mois voire des années, données transmises à des tiers, etc. Les individus faisant usage du réseau et de toute la variété de services en ligne perdent dans une grande mesure la maîtrise de leurs données. Ils ne savent pas ce qui est fait de leurs données, ils ne peuvent contrôler à distance qui y accède. Une série d'acteurs de l'Internet, par contre, connaissent leurs goûts, leurs centres d'intérêt, leurs mouvements, les endroits et les personnes qu'ils fréquentent, etc. Le droit à la protection des données vise à permettre à l'individu de savoir « qui sait quoi » sur lui, de connaître les données le concernant qui sont détenues par d'autres, d'en maîtriser les circuits de communication et d'en contrecarrer les utilisations abusives.

Si ce droit est un instrument de l'épanouissement individuel, il est aussi intimement lié à d'autres droits et libertés qu'il permet d'exercer. C'est parce que l'individu est à l'abri de la surveillance et de l'intrusion d'autorités publiques qu'il peut s'informer sans peur, échanger des informations ou des idées sans arrière-pensée, se mouvoir et circuler librement, s'associer avec d'autres, militer dans l'ombre, etc. Le droit à la protection des données est donc lié au droit à l'information et à la liberté d'expression, ainsi qu'à la liberté de mouvement, au droit à la non-discrimination et au droit à des élections libres.

La Convention 108+ établit clairement ce lien entre la protection des données et les autres droits et libertés.[9] Ainsi aux termes de son article 1er, « [l]e but de la présente Convention est de protéger toute personne physique, quelle que soit sa

---

8 Article 3 Convention 108+: « Champ d'application - 1. Chaque Partie s'engage à appliquer la présente Convention aux traitements de données relevant de sa juridiction dans les secteurs public et privé, **garantissant ainsi à toute personne le droit à la protection de ses données à caractère personnel.** » (c'est nous qui soulignons).
Article 2 RGPD: « Le présent règlement protège les libertés et droits fondamentaux des personnes physiques, et **en particulier leur droit à la protection des données à caractère personnel.** » (c'est nous qui soulignons).

9 *Cécile de Terwangne*, Internet et la protection de la vie privée et des données à caractère personnel, in : Van Enis/de Terwangne (éd.), L'Europe des droits de l'homme à l'heure d'Internet, 2019, 302 ss.

nationalité ou sa résidence, à l'égard du traitement des données à caractère personnel, **contribuant ainsi au respect de ses droits de l'homme et de ses libertés fondamentales, et notamment du droit à la vie privée** ». Le RGPD va dans le même sens puisqu'il stipule dès son article 1er, paragraphe 2, que «[l]e présent règlement **protège les libertés et droits fondamentaux des personnes physiques, et en particulier leur droit à la protection des données à caractère personnel** ».

La loi fédérale suisse du 25 septembre 2020, quant à elle, affirme dès son article 1er que son but consiste à « **protéger la personnalité et les droits fondamentaux** des personnes physiques dont les données personnelles font l'objet d'un traitement ». Si elle ne proclame pas un « droit à la protection des données », elle s'inscrit toutefois bien dans la ligne des textes européens. Au travers des données personnelles, c'est l'ensemble des droits fondamentaux des individus qui sont protégés.

La loi vise aussi expressément à protéger la personnalité des individus dont les données font l'objet d'un traitement. La notion de personnalité doit être comprise, selon le Tribunal fédéral, comme l'ensemble des biens et des valeurs qui appartiennent à une personne du seul fait de son existence, qu'il s'agisse de valeurs physiques, psychiques, morales ou sociales.[10] La personnalité est par ailleurs protégée contre toute atteinte illicite par l'article 28, alinéa 1, du Code civil suisse qui dispose que « [c]elui qui subit une atteinte illicite à sa personnalité peut agir en justice pour sa protection contre toute personne qui y participe ». Le Tribunal fédéral a précisé qu' « [i]l y a atteinte à la personnalité au sens de l'art. 28 CC non seulement lorsque la bonne réputation d'une personne ou son sentiment d'honorabilité sont lésés, mais aussi lorsque sa considération professionnelle ou sociale est touchée. »[11] A travers la législation de protection des données, c'est donc tout à la fois l'honneur, la réputation, l'image, le nom, la vie privée et l'intégrité physique, psychique et morale[12] d'une personne qui sont protégés comme parties intégrantes de la personnalité.

La Convention 108+ affirme en outre le lien entre la protection des données et la protection de la dignité humaine. Dès son préambule, elle déclare « qu'il est nécessaire de garantir la dignité humaine ». Le Rapport explicatif apporte cette précision : « La dignité humaine requiert la mise en place de garanties lors du traitement de données à caractère personnel, afin que les individus ne soient pas traités comme de simples objets. »[13] C'est ainsi au nom de la dignité humaine qu'on ne peut admettre que l'homme soit soumis aux décisions d'une machine. Cette conviction prendra la forme du droit à ne pas être soumis à des décisions entièrement

10 *Yves Burnand*, Le droit de la personnalité, 2006, 4, disponible à l'adresse <http://www.cfjm.ch/wp-content/uploads/2016/02/Burnand_Les_droits_de_la_personnalite%CC%81_29.01.16.pdf>.

11 TF arrêt 5A_170/2013, 5A 174/2013 du 3 octobre 2013, cons. 3.2.

12 *Sylvain Métille*, Le droit au respect de la vie privée : les défis digitaux, une perspective de droit comparé, 2018, 4-13, disponible à l'adresse <https://serval.unil.ch/resource/serval:BIB_25D40801BCE2.P001/REF> ; ARTIAS, Protection de la personnalité et protection contre les discriminations, Guide social romand, 2020, 1-2; *Burnand* (note 10), 4-7.

13 Rapport explicatif du Protocole d'amendement à la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (STE n° 108), 18 mai 2018, § 10.

automatisées, prévu à l'article 9.1.a.[14] de la Convention 108+ ainsi qu'à l'article 22[15] du RGPD, et que l'on retrouve à l'article 21, al. 2[16] de la LPD.

C. Champ d'application personnel, matériel et territorial

I. Secteurs public et privé

La Convention 108+ est applicable à toute activité de traitement de données. Les activités en question peuvent concerner le secteur privé comme le secteur public, ce dernier incluant notamment les domaines de la justice, de la lutte en matière pénale, de la défense, de la sécurité publique et la sûreté de l'Etat. C'est donc l'ensemble des traitements de données à caractère personnel qui sont couverts. Tous les domaines d'activités de l'Etat, des entreprises, des associations ou des individus, dans lesquels il est fait recours à des traitements de données sont visés, même si des exceptions aux dispositions susceptibles d'entraver l'efficacité de l'action dans les domaines de la sécurité et de la justice, ou qui conduiraient à porter atteinte à la séparation des pouvoirs, sont prévues par le texte.[17]

La Convention se distingue du RGPD sur ce point. Le RGPD ne s'applique pas aux traitements de données à caractère personnel se rapportant à des activités relatives à la sécurité nationale car ces activités se situent hors du champ d'application du droit de l'Union européenne.[18] Il est à noter que la Cour de Justice a clarifié dans son arrêt *La Quadrature du Net* ce qui est couvert par la notion de sécurité nationale. Pour la Cour, « [c]ette responsabilité correspond à l'intérêt primordial de protéger les fonctions essentielles de l'État et les intérêts fondamentaux de la société et inclut la prévention et la répression d'activités de nature à déstabiliser gravement les structures constitutionnelles, politiques, économiques ou sociales fondamentales d'un pays, et en particulier à menacer directement la société, la population ou l'État en tant que tel, telles que notamment des activités de terrorisme. »[19]

---

14 « Article 9. Droits des personnes concernées
1. Toute personne a le droit : *a.* de ne pas être soumise à une décision l'affectant de manière significative, qui serait prise uniquement sur le fondement d'un traitement automatisé de données, sans que son point de vue soit pris en compte ».

15 « Article 22. Décision individuelle automatisée, y compris le profilage
1. La personne concernée a le droit de ne pas faire l'objet d'une décision fondée exclusivement sur un traitement automatisé, y compris le profilage, produisant des effets juridiques la concernant ou l'affectant de manière significative de façon similaire. ».

16 « Article 21 Devoir d'informer en cas de décision individuelle automatisée
[...] 2. Si la personne concernée le demande, le responsable du traitement lui donne la possibilité de faire valoir son point de vue. La personne concernée peut exiger que la décision individuelle automatisée soit revue par une personne physique. ».

17 cf. articles 11 et 14.4.c Convention 108+.

18 Article 3.2.a. RGPD; considérant 16 RGPD.

19 CJUE, aff. C-511/218, ECLI:EU:C:2020:791 (La Quadrature du Net e.a.) ; CJUE, aff. Jointes C-623/17, C-511/18 et C-520/18, ECLI:EU:C:2007:383, cons. 135 (Ordre des barreaux francophones et germanophone e.a.).

Le RGPD ne s'applique pas davantage aux activités de traitement effectuées par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, y compris la protection contre les menaces pour la sécurité publique et la prévention de telles menaces et la libre circulation de ces données. La protection des personnes physiques à l'égard du traitement de leurs données à caractère personnel à ces fins est réalisée par le biais d'un instrument juridique spécifique plutôt que par le RGPD : la directive 2016/680 du Parlement européen et du Conseil du 27 avril 2016.[20]

Aux termes de l'article 2 de la LPD, cette loi régit le traitement de données personnelles effectué par des personnes privées ou par des organes fédéraux à l'exception des traitements réalisés par le législateur (les Chambres fédérales et les commissions parlementaires) dans le cadre de ses délibérations et des traitements mis en œuvre par les tribunaux judiciaires.

II. Traitements automatisés et traitements manuels

Concernant le champ d'application matériel, la Convention 108+ s'est alignée sur le RGPD : le champ d'application des deux textes couvre non seulement les traitements de données à caractère personnel entièrement ou partiellement automatisés mais aussi les traitements non automatisés de données à caractère personnel contenues ou appelées à figurer dans un fichier.[21] La protection des données intervient donc dès qu'il y a recours à des technologies de l'information pour traiter des données à caractère personnel, mais aussi lorsque des données sont reprises au sein « d'un ensemble structuré de données qui sont accessibles ou peuvent être retrouvées selon des critères spécifiques »[22] (registre, carnet d'adresses, listing d'entrées, annuaire téléphonique, etc. structuré selon un critère tel l'ordre alphabétique, chronologique ou autre).

La LPD s'applique, quant à elle, à tout traitement de données personnelles sans préciser s'il s'agit de traitement automatisé ou non.[23] Toutefois la définition de « traitement » indique qu'il faut entendre par là « toute opération relative à des données personnelles, quels que soient les moyens et procédés utilisés [...] ».[24] Le fait que la loi couvre tous les traitements de données personnelles quels que soient les moyens ou les procédés utilisés permet d'englober dans son champ d'application toute forme de traitement, y compris les fichiers manuels sur support papier.

---

20 Directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données et abrogeant la décision-cadre 2008/977/JAI du Conseil, L 119/89.

21 Articles 2.b., 2.c. et 3.1. Convention 108+ ; article 2.1 RGPD.

22 Article 2.c. Convention 108+ ; article 4.6. RGPD.

23 Article 2.1. LPD.

24 Article 5.d. LPD.

La notion de fichier qui apparaissait dans l'ancienne loi fédérale suisse de protection des données[25] a été abandonnée avec la disparition de la notion de « maitre du fichier » au profit de celle de « responsable du traitement ». Que ce soit dans ses versions ancienne ou nouvelle, la loi fédérale suisse ne recour(ai)t pas à la notion de fichier pour définir son champ d'application, ce qui a pour conséquence que, en présence de document exclusivement sur support papier, la LPD s'applique dès que des données personnelles apparaissent, sans qu'il soit nécessaire que les données soient structurées. Griffonner un numéro de téléphone professionnel sur un bout de papier, épingler une photo d'équipe sur le mur de la salle des profs ou de la cafétéria de l'entreprise, ou mettre en vitrine des livres dont on voit le nom de l'auteur, correspondent à la réalisation de traitements de données personnelles soumis à la LPD. Par contre, ces exemples de traitement non automatisés n'entrant pas dans la notion de fichier de la Convention 108+ ou du RGPD, ils se trouvent hors du champ d'application de ces deux textes européens.

III. Exclusion des traitements dans le cadre d'activités exclusivement personnelles ou domestiques

Tant la Convention 108+[26] que le RGPD[27] excluent du champ d'application de la protection les traitements de données effectués dans le cadre d'activités exclusivement (ou strictement) personnelles ou domestiques.

Selon le Rapport explicatif de la Convention 108+, il faut entendre par « activités personnelles ou domestiques » « des activités étroitement et objectivement liées à la vie privée d'une personne et qui n'ont pas d'impact significatif sur la sphère personnelle d'autrui. Elles n'ont aucun aspect professionnel ou commercial et sont exclusivement liées à des activités personnelles ou domestiques comme le stockage de photos de famille ou de photos privées sur un ordinateur, la création d'une liste comportant les coordonnées d'amis ou de membres de la famille, ou la correspondance, etc. ».[28] Pour qu'un partage de données puisse être considéré comme effectué au sein de la sphère privée – et dès lors être exclu du champ d'application de la Convention – il faut qu'il ait lieu, par exemple, au sein « de la famille, d'un cercle restreint d'amis ou d'un cercle limité en taille, fondé sur une relation personnelle ou une relation de confiance particulière ».[29]

Le Rapport explicatif précise encore que les données « ne peuvent pas être accessibles à un nombre indéterminé de personnes, ni même à un trop grand nombre, ni enfin à des personnes qui ne présentent pas de lien (familial, affectif ou de connaissance) avec la personne qui traite les données ».[30]

---

25 Article 3.i. Loi fédérale de protection des données du 19 juin 1992. Le fichier correspond à tout ensemble de données personnelles dont la structure permet de rechercher les données par personne concernée.

26 Article 3.2 Convention 108+.

27 Article 2.2.c. RGPD.

28 Paragraphe 27 du Rapport explicatif de la Convention 108+.

29 *Ibidem*.

30 Paragraphe 28 du Rapport explicatif de la Convention 108+.

Dans le même sens, si le considérant 18 du RGPD clarifie que cette exception peut s'appliquer dans le contexte d'Internet, la jurisprudence de la Cour de Justice de l'UE a établi depuis 2003 qu'il faut conserver à la diffusion de données personnelles sur Internet un caractère strictement personnel pour pouvoir invoquer l'exception. Pour cela, les données ne peuvent pas être accessibles à un nombre indéfini et illimité de personnes.[31] Dans de nombreux cas, l'usage des réseaux sociaux, et en particulier de *Facebook* ou *YouTube*, ne répondent pas à cette condition de caractère strictement personnel pour entrer dans l'exception.[32]

Cette exception est également valable hors du contexte d'Internet. Elle peut s'appliquer à la caméra placée dans une maison ou dans la chambre d'un bébé, aux agendas et carnets d'adresses privés, aux listes d'amis invités pour un évènement privé, etc. La Cour de Justice de l'UE a eu l'occasion, le 10 juillet 2018, de réaffirmer que l'exception doit être interprétée comme visant uniquement les activités qui s'insèrent dans le cadre de la vie privée ou familiale des particuliers, soit les activités qui ne dépassent pas la sphère privée.[33] L'exception ne couvre donc pas, par exemple, les traitements de données récoltées à la suite d'action de prédication de porte-à-porte (ce qui était précisément l'objet de l'affaire des Témoins de Jéhovah tranchée en 2018 par la Cour de Justice) ni les captures d'images faites par un drone dans l'espace public, ou par une caméra débordant partiellement sur la voie publique.[34]

Du considérant 18 du RGPD, on peut par ailleurs déduire que, dès qu'un traitement est effectué dans le cadre d'une activité commerciale ou professionnelle, il ne peut être considéré comme poursuivant une finalité « personnelle ou domestique ».

La nouvelle loi suisse de protection des données s'inscrit dans la même ligne que les deux textes européens car elle stipule aux termes de son article 2 let. a qu'elle ne s'applique pas « aux traitements de données personnelles effectués par une personne physique pour un usage exclusivement personnel. » Si la LPD évoque les traitements de données réalisés pour en faire un usage exclusivement personnel, il est clair qu'elle vise la même réalité que les textes européens qui parlent des traitements effectués dans le cadre d'activités exclusivement personnelles ou domestiques.

---

31 Cf. à cet égard : CJUE, aff. C-345/17, ECLI:EU:C:2019:122, cons. 43 (Sergejs Buivids). Également CJUE, aff. C-212/13, ECLI:EU:C:2014:2428 (Ryneš); CJUE, aff. C-73/07, ECLI:EU:C:2008:727, cons. 44 (Satakunnan Markkinapörssi et Satamedia); CJUE, aff. C-101/01, ECLI:EU:C:2003:596, cons. 47 (Lindqvist); *Cécile de Terwangne*, Titre II. Définitions clés et champ d'application du RGPD, in : de Terwangne/Rosier (éd.), Le Règlement général de protection des données (RGPD/GDPR). Analyse approfondie, 2018, 71 ss.

32 Pour un cas d'application sur *YouTube*, cf. CJUE, aff. C-345/17 ECLI:EU:C:2019:122 (Sergejs Buivids).

33 CJUE, aff. C-25/17, ECLI:EU:C:2018:551 (Jehovan todistajat).

34 CJUE, aff. C-212/13, ECLI:EU:C:2014:2428 (Ryneš).

IV. Champ d'application territorial

La Convention 108+ fait référence à la notion de « juridiction » plutôt qu'à celle de « territoire » pour définir son champ d'application. Ainsi, l'article 3, § 1er énonce : « Chaque Partie s'engage à appliquer la présente Convention aux traitements de données **relevant de sa juridiction** dans les secteurs public et privé, garantissant ainsi à toute personne le droit à la protection de ses données à caractère personnel. » Par ailleurs, la Convention modernisée stipule expressément que « [l]e but de la présente Convention est de protéger toute personne physique, **quelle que soit sa nationalité ou sa résidence**, à l'égard du traitement des données à caractère personnel ».[35] La protection est donc offerte dès qu'un traitement de données entre dans la juridiction d'un Etat ou d'une organisation internationale Partie à la Convention, et ce, indépendamment de la nationalité ou du lieu de résidence des personnes physiques dont les données sont traitées.

Quant au RGPD, une de ses caractéristiques les plus remarquables, marquant un changement substantiel par rapport à la directive 95/46, c'est l'étendue de son champ d'application territorial.[36] Ce texte réussit à toucher des acteurs situés hors de l'Union européenne, comme en Suisse, mais actifs sur le marché européen et impactant des personnes localisées dans l'UE. L'article 3 définit le champ d'application territorial sur la base de deux critères principaux: le critère d'« établissement » et le critère de « ciblage ».[37]

Le RGPD est ainsi applicable :

- aux responsables de traitement ou sous-traitants qui ont un établissement sur le territoire de l'UE :[38] pour tous les traitements effectués dans le cadre des activités de cet établissement, que les traitements eux-mêmes aient lieu sur le territoire européen ou non ;
- aux responsables de traitement ou sous-traitants qui ne sont pas établis dans l'UE : pour les traitements qui sont liés à l'offre (gratuite ou contre paiement) de biens ou de services à des personnes concernées se trouvant sur le territoire de l'UE, ou qui sont liés au suivi du comportement de ces personnes, si ce comportement a lieu sur le territoire de l'UE.[39] C'est donc la localisation du public

35 Article 1er Convention 108+.

36 *Cécile de Terwangne/Karen Rosier/Bénédicte Losdyck*, Lignes de force du nouveau règlement relatif à la protection des données à caractère personnel, R.D.T.I. 2016/62, 14, n°12.

37 Cf. Comité européen de la protection des données (EDPB), Lignes directrices 3/2018 relatives au champ d'application territorial du RGPD (article 3), version 2.0, 12 novembre 2019, disponible à l'adresse <https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_3_2018_territorial_scope_fr.pdf>.

38 Cf. *Chloé Ponsart/Romain Robert*, Le règlement européen de protection des données personnelles, J.T. 2018, 423. Sur la notion d'établissement, cf. EDPB, Lignes directrices 3/2018 précitées, 6 ss ; CJUE, aff. C-131/12, ECLI:EU:C:2014:317 (Google Spain) ; *Elise Defreyne/Romain Robert*, R.D.T.I. 2014/56, 53 ss ; CJUE, aff. C-230/14, ECLI:EU:C:2015:639 (Weltimmo) ; *Thierry Léonard/Didier Chaumont*, Article 3 – Champ d'application territorial, gdpr.expert, <https ://www.gdpr-expert.eu/article.html?id=3>.

39 Art. 3.2. RGPD. Pour de plus amples développements sur ces hypothèses, cf. *de Terwangne* (note 31), 75 ss. ; *Ponsart/Robert* (note 38), 423 ; *Fabienne Jault-Seseke*, La portée extraterritoriale ou a-territoriale du RGPD, R.A.E./L.E.A. 2018/1, 43 ss.

cible du traitement des données qui est le critère déterminant dans ce cas. Et l'intention de viser ce public cible peut être établie à partir d'indicateurs comme l'utilisation d'une langue ou d'une monnaie d'un État membre.[40]

Les acteurs localisés hors de l'Union doivent désigner un représentant établi sur le territoire de l'Union,[41] sauf si le responsable du traitement est une autorité publique ou un organisme public ou encore lorsque le traitement ne présente pas vraiment de risque. Dans le même esprit que cet article 3 du RGPD, et dans la ligne de la jurisprudence du Tribunal fédéral dans l'affaire *Google Street View*, la LPD s'applique, aux termes de son article 3, aux états de fait qui déploient des effets en Suisse, même s'ils se sont produits à l'étranger. Formulée de la sorte, cette disposition risque de soulever à l'avenir des questions d'interprétation.

D. Définitions

I. Donnée à caractère personnel

Comme par le passé, la « donnée à caractère personnel » est définie comme toute information qui concerne une personne physique identifiée ou identifiable (appelée la « personne concernée »).[42] La LPD reprend, elle aussi, cette définition,[43] laissant tomber les personnes morales auparavant couvertes par la protection des données. La loi conserve l'expression simplifiée – bienvenue – de « donnée personnelle » qui était déjà présente dans la version de 1992.

La notion de donnée à caractère personnel est particulièrement large puisqu'elle englobe n'importe quel type d'informations, qu'il s'agisse d'informations privées et confidentielles, d'informations professionnelles, d'informations objectives ou subjectives, ou encore d'informations publiques, diffusées par exemple sur le Web.[44] Toute forme d'information est par ailleurs couverte. Les données peuvent ainsi prendre la forme d'écrits, d'images (photos, vidéos), de sons, il peut s'agir de données de localisation, de données de comportement en ligne, de données biométriques, etc.

N'entrent dans le champ de la Convention 108+ et du RGPD que les données à caractère personnel concernant une personne physique vivante.[45]

---

40 En revanche, « la simple accessibilité du site internet du responsable du traitement, d'un sous-traitant ou d'un intermédiaire dans l'Union, d'une adresse électronique ou d'autres coordonnées, ou l'utilisation d'une langue généralement utilisée dans le pays tiers où le responsable du traitement est établi ne suffit pas pour établir cette intention » (Considérant 23 RGPD).

41 Art. 27 du RGPD.

42 Article 2.a. Convention 108+; Article 4.1 RGPD.

43 Article 5.a. LPD.

44 CJUE, aff. C-73/07, ECLI:EU:C:2008:727, cons. 49 (Satakunnan Markkinapörssi et Satamedia); pour de plus amples développements sur les différents types de données couverts, cf. *de Terwangne* (note 31), 71 ss.

45 Cf. Paragraphe 30 du Rapport explicatif de la Convention 108+; considérant 27 RGPD.

La personne concernée par l'information doit être identifiée ou à tout le moins identifiable pour qu'on puisse parler de « données à caractère personnel ». L'identification dont il est question doit se comprendre non comme l'établissement de l'identité civile d'un individu mais comme **l'individualisation** de cette personne, la capacité de la distinguer et la traiter différemment des autres, de la masse.[46] Un glissement s'est opéré de la notion d'identification vers un concept d'individualisation. Cette individualisation peut se faire, par exemple, en se référant au nom de la personne directement mais également à partir « d'un numéro d'identification, d'un pseudonyme, de données biométriques ou génétiques, de données de localisation, d'une adresse IP ou d'un autre identifiant, qui renvoient à une personne donnée ou à un appareil ou un ensemble d'appareils (ordinateur, téléphone portable, appareil photo, console de jeux, etc.) ».[47]

Si l'identification du sujet des données nécessite des délais, des efforts ou des ressources déraisonnables, ce sujet ne sera plus à considérer comme étant « identifiable » et les données se rapportant à lui seront réputées anonymes. Ce qui représente des délais, efforts ou ressources déraisonnables doit s'analyser au cas par cas, « en tenant notamment compte de l'objet du traitement et de critères objectifs tels que le coût, les bénéfices d'une telle identification, le type de responsable du traitement ou la technologie employée, etc. ».[48] En outre, les avancées technologiques peuvent faire fluctuer ce qui doit être considéré comme « délais, efforts ou ressources déraisonnables ».

Les textes européens ne couvrent pas les données (rendues) anonymes mais le RGPD différencie ces données des données pseudonymisées[49] – ou codées – qui, quant à elles, sont couvertes par la protection comme les autres données à caractère personnel.[50]

II. Traitement (de données)

Le traitement vise les opérations appliquées aux données à caractère personnel. La notion de « traitement de données » a pris la place dans la Convention 108+[51] de celle de « fichier automatisé » utilisée dans le texte initial mais qui ne correspondait plus

46 Paragraphe 18 du Rapport explicatif de la Convention 108+ ; considérant 26 RGPD.

47 Paragraphe 18 du Rapport explicatif de la Convention 108+. Egalement article 4.1. RGPD et considérant 30 RGPD.

48 Paragraphe 17 du Rapport explicatif de la Convention 108+. Sur ce point dans la LPD, cf. *Sylvain Métille*, Le traitement de données personnelles sous l'angle de la (nouvelle) loi fédérale sur la protection des données du 25 septembre 2020, SJ 2021, 5.

49 Définies à l'article 4.5 du RGPD.

50 Considérant 26 du RGPD.

51 Article 2.b. Convention 108+ : Le « traitement de données » « s'entend de toute opération ou ensemble d'opérations effectuées sur des données à caractère personnel, telles que la collecte, l'enregistrement, la conservation, la modification, l'extraction, la communication, la mise à disposition, l'effacement ou la destruction des données, ou l'application d'opérations logiques et/ou arithmétiques à ces données ».

aux réalités technologiques actuelles. Cette notion est équivalente à celle, raccourcie, de « traitement » adoptée dans le RGPD[52] ainsi que dans la LPD.

Il est à noter que la LPD donne du traitement une vision éclatée, opération par opération, et non une vue d'ensemble des opérations effectuées sur des données. La loi définit en effet le traitement comme « toute opération relative à des données personnelles, quels que soient les moyens et procédés utilisés, notamment la collecte, l'enregistrement, la conservation, l'utilisation, la modification, la communication, l'archivage, l'effacement ou la destruction de données ».[53] Une telle définition faisant de chaque opération distincte un traitement pose problème dans la pratique, par exemple lorsque la LPD impose de tenir un registre des activités de traitement où l'on doit spécifier notamment la finalité de chaque traitement effectué. Il est vrai qu'une opération isolée peut déjà constituer un traitement, mais le plus souvent il s'agira d'un ensemble d'opérations appliquées à des données. Ce qui permet de lier ces opérations pour les considérer comme formant un seul traitement c'est la finalité qui est poursuivie par cet ensemble d'opérations (traitement de gestion de la clientèle, traitement de paiement des salaires, traitement de marketing, traitement de suivi du patient, etc.).

III. Responsable du traitement

Selon l'article 2, c, de la Convention 108+, la notion de responsable du traitement signifie « la personne physique ou morale, l'autorité publique, le service, l'agence ou tout autre organisme qui, seul ou conjointement avec d'autres, dispose du pouvoir de décision à l'égard du traitement de données ». Aux termes de l'article 4.7 du RGPD, le responsable du traitement est celui « qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement ».

Ainsi, alors que cet acteur principal est identifié dans le RGPD comme étant la personne compétente pour décider de la finalité du traitement et des moyens à mobiliser, il est recouru dans la Convention 108+ à un critère moins détaillé mais destiné à éclairer davantage sur le rôle décisif du responsable du traitement à l'égard du traitement effectué sur les données. C'est donc la personne qui exerce le pouvoir de décision sur ce traitement. Ce pouvoir de décision peut porter sur les motifs justifiant le traitement, à savoir ses finalités, ainsi que sur les moyens utilisés pour traiter les données. On peut également tenir compte du fait de contrôler ou non les méthodes du traitement, le choix des données à traiter et les personnes autorisées à y accéder.[54]

---

52 L'article 4.2 du RGPD définit ainsi le traitement : « toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données ou des ensembles de données à caractère personnel, telles que la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation, l'effacement ou la destruction ».

53 Article 5.d. LPD.

54 Paragraphe 22 Rapport explicatif de la Convention 108+.

Le législateur suisse a repris textuellement la définition du RGPD, apportant la précision qu'il peut s'agir d'une personne privée ou d'un organe fédéral.[55]

L'identification du responsable du traitement peut découler d'une désignation officielle ou de circonstances factuelles à apprécier au cas par cas.[56]

Il est encore à noter que la qualité de responsable du traitement peut être partagée. Dans le cas où différents intervenants définissent les finalités ou les moyens du traitement, on sera en présence de plusieurs co-responsables de ce traitement.[57] Il est alors question de responsables conjoints.[58] Cette responsabilité conjointe ne signifie pas nécessairement une responsabilité équivalente des différents intervenants. Ceux-ci peuvent être impliqués à différents stades ou être en charge de différents aspects du traitement.[59]

IV. Sous-traitant

La Convention 108+ comme le RGPD confient[60] des responsabilités spécifiques à un acteur dont le rôle s'est accru depuis son apparition dans la directive 95/46 : le sous-traitant, c'est-à-dire la personne physique ou morale, l'autorité publique, le service, l'agence ou tout autre organisme qui traite des données à caractère personnel pour le compte du responsable du traitement.[61] La LPD a repris cette notion et vise par là « la personne privée ou l'organe fédéral qui traite des données personnelles pour le compte du responsable du traitement ».[62]

Il s'agit donc de la personne, au sens large, qui travaille pour le compte du responsable du traitement, pour effectuer les tâches (généralement techniques) que ce responsable n'est pas à même d'effectuer et qu'il lui délègue. Le sous-traitant est une personne extérieure au responsable du traitement ; il ne peut s'agir d'un employé de ce dernier. Il doit accomplir les opérations de traitement conformément

55 Article 5.j. LPD.

56 Paragraphe 22 Rapport explicatif de la Convention 108+.

57 Paragraphe 22 Rapport explicatif de la Convention 108+ ; article 4.7 RGPD ; cf. *Antoine Delforge*, Les obligations générales du responsable du traitement et la place du sous-traitant, in : de Terwangne/Rosier (éd.), Le règlement général sur la protection des données (RGPD/GDPR), Analyse approfondie, 2018, 381 ss.

58 Article 26 RGPD. La CJUE a par exemple considéré que l'administrateur d'une *Fan page* était responsable conjoint de certains traitements de données avec *Facebook*. Cf. CJUE, aff. C-210/16, ECLI:EU:C:2018:388 (Wirtschaftsakademie Schleswig-Holstein); CJUE, aff. C-40/17, ECLI:EU:C:2019:629 (Fashion ID).

59 Paragraphe 22 Rapport explicatif de la Convention 108+ CJUE, aff. C-210/16, ECLI:EU:C:2018:388, cons. 43 (Wirtschaftsakademie Schleswig-Holstein); Pour les conséquences découlant du statut de responsables conjoints, cf. *Bojana Salovic/Thierry Léonard/Etienne Wery*, Bouton « J'aime » de Facebook : voici le verdict final de la CJUE, 29 juillet 2019, <https://www.droit-technologie.org/actualites/bouton-jaime-de-facebook-voici-le-verdict-final-de-la-cjue/>.

60 Article 10 Convention 108+ ; article 28 RGPD.

61 Article 2.f Convention 108+; Article 4.8 RGPD.

62 Article 5.k LPD.

aux instructions du responsable du traitement. Ces instructions tracent les limites de l'utilisation autorisée des données à caractère personnel par le sous-traitant.[63]

E. Principes

I. Exigence de proportionnalité du traitement des données

L'exigence de proportionnalité du traitement des données est proclamée solennellement à l'article 5, §1, de la Convention 108+. Par contre, elle n'est pas énoncée en tant que telle dans le RGPD mais elle est abondamment formulée dans la jurisprudence de la Cour de Justice.[64]

Aux termes de l'article 5.1 de la Convention 108+, « le traitement de données doit être proportionné à la finalité légitime poursuivie et refléter à chaque étape du traitement un juste équilibre entre tous les intérêts en présence, qu'ils soient publics ou privés, ainsi que les droits et les libertés en jeu ». Tout traitement de données doit donc être proportionné, c'est-à-dire pertinent au regard de la finalité légitime poursuivie et limité à ce qui est nécessaire au regard des intérêts, droits et libertés des personnes concernées ou de l'intérêt public. Il ne doit pas induire une ingérence disproportionnée dans ces intérêts, droits et libertés.[65]

L'article 5.1 de la Convention 108+ est assurément une des dispositions les plus importantes de ce texte. Il peut jouer un rôle crucial face au développement de traitements de données qui mettent à mal l'équilibre entre quête d'efficacité et protection des droits et libertés (dans le secteur public) ou entre intérêts économiques et protection de ces mêmes droits et libertés (dans le secteur privé). Dès lors que l'on va toujours plus loin dans le « techniquement possible » et que les intérêts économiques liés à l'exploitation des données à caractère personnel sont toujours plus grands, cette disposition impose de réfléchir à l'acceptabilité des systèmes d'information et des utilisations des données envisagés. C'est aussi cette disposition qui permet de sortir d'une approche individualiste, de dépasser l'intérêt

63 Paragraphe 24 du Rapport explicatif de la Convention 108+.

64 CJUE, aff. jointes C-92/09 et C-93/09, ECLI:EU:C:2010:662, cons. 77 (Volker und Markus Schecke et Eifert) ; CJUE, aff. jointes C-293/12 et C-594/12, ECLI:EU:C:2014:238, cons. 52 (Digital Rights Ireland e.a.*)*; CJUE, aff. C-362/14, ECLI:EU:C:2015:650, cons. 92 (Schrems); CJUE, aff. jointes C-203/15 et 698/15, ECLI:EU:C:2016:970, cons. 94 ss (Tele2 Sverige); CourEDH, S. et Marper/Royaume-Uni Requête nos 30562/04 et 30566/04, Recueil 2008, cons. 118.

65 Paragraphe 40 du Rapport explicatif de la Convention 108+. La jurisprudence de la Cour européenne des droits de l'homme va dans le même sens : dans son arrêt *S. et Marper*, la Cour a ainsi affirmé que le traitement de données doit être proportionné, c'est-à-dire approprié par rapport aux buts légitimes poursuivis, nécessaire dans la mesure où il n'existe pas d'autres mesures appropriées moins attentatoires aux intérêts, droits et libertés des personnes concernées ou de la société, et qu'il ne peut induire une atteinte démesurée à ces intérêts, droits et libertés par rapport aux bénéfices attendus par le responsable du traitement (CourEDH, S. et Marper/Royaume-Uni Requête nos 30562/04 et 30566/04, Recueil 2008, cons. 118).

individuel, et qui invite à mettre dans la balance les intérêts publics, collectifs en jeu.

L'article 5.1. précise que le principe de proportionnalité doit être respecté à toutes les étapes du traitement, à commencer donc par le stade initial, c'est-à-dire lorsqu'il est décidé de procéder ou non au traitement des données,[66] et ensuite lors de chaque opération effectuée sur les données, notamment lors de leur utilisation, de leur communication à un tiers ou de leur interconnexion avec d'autres données.

Il est donc désormais particulièrement clair qu'il faut mettre en balance l'ensemble des droits et libertés en jeu avant le lancement de tout traitement de données, et que les opérations ne peuvent être faites sur des données que si le résultat de la mise en balance est équilibré. Et cela, même si on a obtenu le consentement des personnes concernées. En effet, comme le Rapport explicatif le signale, « [l]'expression d'un consentement ne dispense pas de respecter les principes fondamentaux de la protection des données à caractère personnel énoncés au chapitre II de la Convention : la proportionnalité du traitement, par exemple, doit toujours être considérée. »[67] Ainsi donc, l'exigence de proportionnalité peut servir de rempart non seulement face aux risques de certains développements (comme les traitements de données insoupçonnés qui foisonnent sur Internet) mais aussi face au recours très (abusivement ?) répandu au consentement des personnes concernées pour traiter leurs données. Si la présence d'un consentement permet de présumer la légitimité d'un traitement, la mise en balance des intérêts en présence et la vérification de l'équilibre atteint offre une sauvegarde bienvenue quand on songe aux défauts trop souvent attachés au consentement (information insuffisante de la personne concernée, manifestation du consentement déduite de la non-modification de conditions par défaut, etc.). De plus, le consentement exprimé par la personne concernée ne reflète que la prise en compte de ses intérêts, droits et libertés propres et non de ceux d'autrui ou de la collectivité. Ce que l'un est prêt à accepter par facilité ou intérêt économique n'est peut-être pas souhaitable à l'échelle de la société dans son ensemble. On pourrait dès lors contester un tel traitement de données au nom du non-respect de l'exigence de proportionnalité.

Au vu de ce qui précède, on peut saluer le fait que la LPD accorde expressément, elle aussi, une place au principe de proportionnalité. Aux termes de son article 6 al. 2, « [t]out traitement de données personnelles doit être conforme aux principes de la bonne foi et de la proportionnalité ».

De l'intégration de ce principe dans la législation suisse de protection des données découlent des exigences quant aux données pouvant être traitées : seules les données nécessaires pour atteindre le but fixé peuvent faire l'objet du traitement.[68] Mais ce principe dépasse la seule question des données collectées, il s'applique également « aux types et aux catégories de données traitées, aux moyens de traitement, aux finalités, à la durée de conservation, etc. »[69]

---

66 *Ibidem*.

67 Paragraphe 44 du Rapport explicatif de la Convention 108+.

68 *Métille* (note 48), 9; *Philippe Meier*, Protection des données – Fondements, principes généraux et droit privé, 2011, n° 671-675.

69 *Métille* (note 48), 9; *Meier* (note 68), n° 676.

II. Exigence d'un traitement licite

Les données à caractère personnel doivent être traitées de manière licite.[70] Cette exigence de licéité signifie que le traitement de données à caractère personnel doit se faire conformément à l'ensemble des règles légales applicables. Cela implique le respect des règles de protection des données, mais également de toute autre exigence légale qui trouverait à s'appliquer à une situation de traitement de données, comme par exemple les obligations en matière de droit du travail ou de protection du consommateur.

Le RGPD ayant intitulé son article 6 « Licéité des traitements », cela a donné une portée nouvelle à l'exigence de licéité. En plus de ce qui est dit ci-dessus, la licéité implique donc, dans le cadre de ce texte, de disposer d'une des bases énoncées à l'article 6 (consentement, contrat, base légale, ...). La Convention 108+ ne va pas dans cette direction puisqu'elle évoque à son article 5.2 des bases de légitimité plutôt que de licéité des traitements de données.

La LPD a repris l'exigence de licéité à son article 6 al. 1. qui stipule que « [t]out traitement de données personnelles doit être licite. » Le Préposé fédéral à la protection des données et à la transparence a apporté cette précision : « On considère que des données ont été collectées de façon illicite lorsqu'elles ont été obtenues par la force, par la ruse, par la menace ou par la tromperie. »[71] Notons que le recours à la ruse et à la tromperie relève tout autant de la question de la loyauté de la collecte qui est évoquée au point suivant.

III. Principe de loyauté et transparence

Tant la Convention 108+ que le RGPD exigent que « [l]es données à caractère personnel faisant l'objet d'un traitement soient traitées loyalement et de manière transparente »,[72] le RGPD précisant « ... au regard de la personne concernée ».[73] L'exigence de loyauté induit que le traitement des données soit réalisé dans la transparence pour les personnes concernées, et sans tromperie. Les traitements de données ne peuvent se faire à l'insu des personnes sur qui portent les données, d'une manière qui serait tout à fait inattendue ou imprévisible pour elles.

Cette obligation de loyauté se retrouve dans la LPD sous la forme du principe de la bonne foi. En exigeant que tout traitement de données personnelles soit conforme au principe de la bonne foi,[74] la LPD interdit de traiter des données à l'insu de la personne concernée[75] ou de laisser cette dernière penser qu'elle est tenue de fournir ses données alors que la collecte est facultative.[76]

---

70 Article 5.3. Convention 108+; Article 5.1.a. RGPD.

71 PFPDT, Guide pour le traitement des données personnelles dans le secteur privé et Guide pour le traitement des données personnelles dans l'administration fédérale, 2009, 4.

72 Article 5.4.a. Convention 108+.

73 Article 5.1.a. RGPD.

74 Article 6.2. LPD.

75 *Métille* (note 48), 8; *Meier* (note 68), n° 644.

76 *Métille* (note 48), 8.

IV. Principe de finalité

Véritable pierre angulaire de la protection des données, le principe de finalité exige que les données soient collectées pour des finalités déterminées, explicites et légitimes, et ne soient pas traitées ultérieurement de manière incompatible avec ces finalités.[77] Les finalités du traitement des données doivent donc être fixées et claires dès le début. La référence à des « finalités déterminées » indique qu'il n'est pas permis de traiter des données pour des finalités non définies, imprécises ou vagues.[78] Pour que les finalités soient légitimes, elles ne peuvent induire une atteinte disproportionnée aux droits, libertés et intérêts en jeu, au nom des intérêts poursuivis par le responsable du traitement.[79]

On peut effectuer sur ces données toutes les opérations qui seront considérées comme compatibles avec les finalités d'origine, c'est-à-dire qui entrent dans les attentes raisonnables des intéressés du fait du lien qu'elles présentent avec la finalité initiale ou du contexte.[80]

La LPD reprend presque textuellement ce principe puisqu'elle stipule à son article 6 al. 3. que « [l]es données personnelles ne peuvent être collectées que pour des finalités déterminées et reconnaissables pour la personne concernée et doivent être traitées ultérieurement de manière compatible avec ces finalités. » Le législateur fédéral a préféré le terme « reconnaissables » à « explicites », ce qui vise vraisemblablement la même chose,[81] même si l'on peut regretter le caractère plus flou et sans doute moins exigeant de ce terme.

Par contre, il n'est pas exigé que les finalités du traitement des données soient légitimes. En fait, étant donné que, pour que la finalité du traitement de données soit légitime, il faut ménager un juste équilibre entre les droits et intérêts de la personne concernée et ceux du responsable du traitement ou de la société,[82] on retrouve au travers de l'adjectif « légitime », l'exigence de proportionnalité existant pour l'ensemble du traitement des données (cf. *suppra* I.). Il n'était donc pas nécessaire de reproduire au niveau des finalités l'exigence de proportionnalité qui vaut pour tous les aspects d'un traitement de données.

V. Exigences de minimisation des données et de limitation de la conservation des données

Aux termes des articles 5.4.c. de la Convention 108+ et 5.1.c, du RGPD, les données à caractère personnel faisant l'objet d'un traitement doivent être adéquates et

77 Article 5.4.b. Convention 108+ ; Article 5.1.b. RGPD.

78 Paragraphe 48 du Rapport explicatif de la Convention 108+.

79 *Ibidem* ; cf. égal. *Marie-Helene Boulanger/Thierry Léonard/Sophie Louveaux/Damien Moreau/Cécile de Terwangne/Yves Poullet*, La protection des données à caractère personnel en droit communautaire, J.T. - droit européen 1997, 145.

80 Cf. article 6.4 et considérant 50 RGPD.

81 Message concernant la loi fédérale sur la révision totale de la loi fédérale sur la protection des données et sur la modification d'autres lois fédérales, FF 2017 6565, 6645 (cf. notamment les exemples donnés par le législateur pour illustrer les finalités reconnaissables).

82 Paragraphe 48 du Rapport explicatif de la Convention 108+.

pertinentes au regard des finalités du traitement. Elles doivent en outre être « non excessives » pour la Convention 108+, ou « limitées à ce qui est nécessaire » pour le RGPD, ce qui doit se comprendre en termes quantitatifs (pas trop de données) et qualitatifs (pas de données qui portent excessivement atteinte à la personne concernée).[83] Cette exigence de minimisation des données conduit à ce que l'on ne puisse traiter des données à caractère personnel que lorsqu'il n'y a pas raisonnablement moyen d'atteindre la finalité sans cela.[84]

Les données ne peuvent être conservées sous une forme permettant l'identification des personnes concernées que « pendant une durée n'excédant pas celle nécessaire aux finalités pour lesquelles elles sont traitées ».[85] Il est précisé au considérant 39 du RGPD que cela implique en outre que la durée de conservation des données soit limitée « au strict minimum ».

La LPD ne reprend explicitement que cette dernière exigence portant sur la durée de conservation des données puisqu'elle exige que les données traitées soient « détruites ou anonymisées dès qu'elles ne sont plus nécessaires au regard des finalités du traitement. »[86] Les autres aspects de la minimisation des données sont couverts par le principe de proportionnalité[87] exposé ci-avant (cf. *suppra* I.).

VI. Exigence de qualité des données

Les données à caractère personnel doivent être exactes et, si nécessaire, mises à jour.[88] Toute inexactitude doit être corrigée, l'article 5, § 1er, d, du RGPD apportant cette précision que la rectification doit être faite « sans tarder ». Il s'agit d'une « obligation de moyens en vertu de laquelle le responsable du traitement doit mettre en œuvre des mesures raisonnables afin de tenir à jour les données qu'il traite ». [89]

Dans le même sens, l'article 6.5. de la LPD stipule que « [c]elui qui traite des données personnelles doit s'assurer qu'elles sont exactes. » Cette disposition instaure clairement une obligation de moyen qu'elle fait peser sur celui qui traite des données car elle signale que ce dernier doit prendre « toute mesure appropriée permettant de rectifier, d'effacer ou de détruire les données inexactes ou incomplètes au regard des finalités pour lesquelles elles sont collectées ou traitées. Le caractère approprié de la mesure dépend notamment du type de traitement et de son étendue, ainsi que du risque que le traitement des données en question présente pour la personnalité ou les droits fondamentaux des personnes concernées. »

83 Paragraphe 52 du Rapport explicatif de la Convention 108+.
84 Considérant 39 RGPD.
85 Article 5.4.e. Convention 108+; article 5.1.e. RGPD.
86 Article 6.4. LPD.
87 *Métille* (note 48), 9.
88 Article 5.4.d Convention 108+ ; article 5.1.d. RGPD.
89 *Ponsart/Robert* (note 38), 424.

F. Légitimité/licéité du traitement

Chaque traitement de données doit reposer sur un fondement légitime.[90] La formulation de cette exigence varie entre les deux textes européens puisque, pour la Convention 108+, un traitement doit avoir une base de légitimité (*legitimacy basis,* dans la version anglaise du texte), tandis que pour le RGPD, le traitement doit remplir une condition de licéité (*lawfulness condition*).

Selon l'article 5.2. de la Convention 108+, le traitement de données ne peut être effectué « que sur la base du consentement libre, spécifique, éclairé et non-équivoque de la personne concernée ou en vertu d'autres fondements légitimes prévus par la loi ». Le Rapport explicatif précise que les « autres fondements légitimes prévus par la loi » englobent « notamment le traitement de données nécessaire à l'exécution d'un contrat (ou de mesures précontractuelles, à la demande de la personne concernée) auquel la personne concernée est partie ; à la protection d'intérêts vitaux de la personne concernée ou d'une autre personne ; à la mise en conformité avec une obligation légale incombant au responsable du traitement ; ainsi que le traitement de données réalisé pour des motifs d'intérêt public ou pour des intérêts légitimes prédominants du responsable du traitement ou d'un tiers ».[91]

Quant au consentement, pour être valable il doit être spécifique, libre, éclairé et non équivoque. Pour que le consentement soit considéré comme libre, aucune influence ou pression indues (de nature économique ou autre) ne peut être exercée sur la personne concernée qui doit disposer d'un véritable choix et doit pouvoir refuser ou retirer son consentement sans subir de préjudice.[92] La personne concernée doit par ailleurs avoir reçu l'information nécessaire sur l'étendue et l'implication de son consentement.[93] Non équivoque, le consentement doit se manifester par le biais d'une déclaration (écrite, électronique ou orale) ou d'une action affirmative qui indique clairement l'acceptation du traitement des données en cause. En conséquence, « le silence, l'inaction ou des formulaires ou cases à cocher prévalidés ne peuvent constituer un consentement ».[94] En outre, le consentement couvre l'ensemble des opérations de traitement de données qui poursuivent la même finalité de sorte que « lorsque les finalités sont multiples, un consentement doit être donné pour chacune d'entre elles ».[95]

Le RGPD formule dans le texte même de son article 6, paragraphe 1, les six hypothèses de licéité des traitements qui correspondent à celles listées dans le Rapport explicatif de la Convention 108+. Par ailleurs, pour être valable aux yeux du RGPD, le consentement donné par la personne concernée pour le traitement de ses données doit répondre aux mêmes conditions[96] que celles énoncées dans la Con-

90 Article 5.2. Convention 108+; article 6.1. RGPD.
91 Paragraphe 46 Rapport explicatif de la Convention 108+.
92 Paragraphes 42 et 45 Rapport explicatif de la Convention 108+.
93 Paragraphe 42 Rapport explicatif de la Convention 108+.
94 *Ibidem*.
95 *Ibidem*.
96 Les conditions de validité du consentement sont énoncées dans la définition donnée du consentement à l'article 4.11 RGPD. Cf. aussi article 7 et considérants 32, 42 et 43 RGPD.

vention 108+. Ajoutons que le RGPD précise que le consentement ne sera pas admis comme libre lorsque l'exécution d'un contrat est suspendue au consentement pour le traitement de données qui ne sont pas nécessaires à ce contrat.[97] De même, le consentement est présumé ne pas être libre en matière d'emploi, vu le déséquilibre existant entre les parties.[98]

Notons encore que pour les hypothèses où la base de légitimité/licéité du traitement de données est la nécessité de conformité avec une obligation légale à laquelle le responsable du traitement est soumis, la base légale doit répondre aux exigences que la Cour européenne des droits de l'homme a fait découler de l'article 8 CEDH : la norme doit être accessible et prévisible. Pour être prévisible, une norme doit être suffisamment détaillée pour qu'à sa lecture, on soit à même d'envisager les traitements de données qui auront lieu.

La LPD n'admet les traitements de données effectués par les personnes publiques que s'il existe une base légale. Cette base légale doit être en principe prévue dans une loi au sens formel ou matériel selon les hypothèses mentionnées dans la LPD.[99]

Pour les traitements effectués par des personnes privées, la LPD ne requiert pas directement que les traitements de données reposent sur une base de légitimité. Toutefois, elle spécifie que « Celui qui traite des données personnelles ne doit pas porter une atteinte illicite à la personnalité des personnes concernées. »[100] Or, pour la loi suisse, selon le Préposé fédéral à la protection des données et à la transparence, « [t]out traitement de données personnelles constitue une atteinte à la personnalité »,[101] sauf lorsque la personne concernée a rendu elle-même volontairement ses données accessibles à tous et ne s'est pas opposée expressément au traitement de ses données.[102] Un traitement de données personnelles réalisera une atteinte illicite à la personnalité s'il n'est pas justifié « par le consentement de la personne concernée, par un intérêt privé ou public prépondérant, ou par la loi. »[103] On retrouve donc indirectement une exigence de justification des traitements de données sur la base du consentement de la personne concernée, d'un intérêt prépondérant public ou privé (ce qui englobe l'exécution d'un contrat[104]) ou de la loi.

Cette lecture de la LPD, qui semble la plus logique, ne correspond toutefois pas totalement au texte même de la loi. Ainsi, il n'y est pas dit expressément que tout traitement réalise une atteinte à la personnalité. Au contraire, l'article 30 al. 2 stipule que « Constitue notamment une atteinte à la personnalité le fait de: a. traiter des données personnelles en violation des principes définis aux art. 6 et 8 ; [...] ». Ce qui peut laisser à penser que si l'on respecte les principes de base des articles 6

97 Article 7.4 et considérant 43 RGPD.

98 Considérant 43 RGPD.

99 Article 34.2 et 34.3 LPD. Des exceptions à cette exigence de base légale sont prévues au paragraphe 4 de l'article 34 LPD.

100 Article 30.1 LPD.

101 PFPDT, Guide pour le traitement des données personnelles dans le secteur privé, 2009, 4.

102 Article 30.3 LPD.

103 Article 31 LPD.

104 Article 31. 2 « Les intérêts prépondérants du responsable du traitement entrent notamment en considération dans les cas suivants: a. le traitement est en relation directe avec la conclusion ou l'exécution d'un contrat et les données traitées concernent le cocontractant […]».

et 8 (proportionnalité, bonne foi, finalité, sécurité, etc.), on ne réalise aucune atteinte à la personnalité et on n'a dès lors pas besoin de base de justification.[105] Cette conclusion est sans doute très théorique car dans la pratique, le respect du principe de proportionnalité conduira à ce que le traitement aura toujours au moins la base de justification de l'intérêt privé ou public prépondérant, si on n'a pas le consentement des personnes concernées. Ce qui fait qu'il ne doit pas y avoir vraiment de situations où le traitement de données respecte tous les principes (y compris la proportionnalité) mais n'aurait aucune des quatre bases de justification. Signalons enfin que la liste des exemples d'atteintes à la personnalité énoncés à l'article 30 al. 2 n'est pas exhaustive puisque l'article dit « notamment ». L'hypothèse mentionnée par le Préposé fédéral (selon lequel tout traitement réalise une atteinte à la personnalité) peut donc se glisser dans la liste par cette ouverture.

On ajoutera encore que l'article 6 al. 6 de la LPD précise que le consentement n'est valable que si la personne concernée « exprime **librement** sa volonté concernant un ou plusieurs traitements **déterminés** et après avoir été dûment **informée** ». Cette disposition contient donc trois conditions identiques à celles énoncées dans la Convention 108+ et le RGPD : le consentement doit être libre, spécifique et éclairé. L'article 6 al. 7 de la LPD ajoute que le consentement doit en outre être **exprès** en présence de données sensibles ou lorsque le traitement des données est lié à un profilage à risque élevé effectué par une personne privée ou à un profilage effectué par un organe fédéral. N'est donc pas explicitement reprise dans la loi suisse la condition que, en toutes circonstances, le consentement soit non équivoque c'est-à-dire qu'il soit manifesté par le biais d'une déclaration ou d'une action affirmative.

---

105 Cf. *Pablo Alonso/Rémi Pactat/Julien Gassmann*, Suisse : enfin une nouvelle loi sur la protection des données, <https://www.wavestone.com/fr/insight/suisse-nouvelle-loi-sur-protection-donnees/> ; *Métille* (note 48), 32 : « en droit suisse le consentement n'est requis que s'il y a une atteinte à la personnalité. [...] des données traitées sans lien avec un contrat mais dans le respect des principes (pas de consentement nécessaire), [...] les données sont traitées en violation des principes (ce qui a nécessité un consentement) ».
Par ailleurs, on pourrait aussi déduire des dispositions de la LPD que l'on peut ne pas respecter les principes si l'on a une base de justification. Or, c'est clairement contraire à la volonté du législateur. Cf. ce qui a été dit en ce sens par le PFPDT à propos de la LPD de 1992 lors de sa modification en 2004 et 2006 (PFPDT, Explications sur les modifications du 17 décembre 2004 et du 24 mars 2006 de la loi fédérale sur la protection des données (LPD), 12) : « Prise à la lettre, cette disposition laisse supposer que sur la base d'un motif justificatif, il est possible de traiter des données en violation du principe de la bonne foi, de manière illicite ou disproportionnée, qu'il est possible de traiter des données fausses ou de renoncer à prendre des mesures techniques et organisationnelles pour éviter que des tiers non autorisés puissent avoir accès à ces données. Une telle interprétation était choquante et ne correspondait pas à la pratique et à l'esprit de la loi. » La modification de la loi à l'époque était censée répondre à ce problème mais on observe que le problème persiste dans le texte de 2020. Il serait sans doute opportun de mettre le texte des articles 30 et 31 de la LPD de 2020 en totale adéquation avec l'intention du législateur. Cela permettrait en outre d'éviter l'étrangeté relevée par *Sylvain Métille* à propos du droit à la remise des données (art. 28 LPD) qui n'est valable que si le traitement s'appuie sur le consentement ou sur la nécessité contractuelle, c'est-à-dire selon la lecture à la lettre de la loi, « lorsque les données sont traitées en violation des principes (ce qui a nécessité le consentement) » ; *Métille* (note 48), 32.

G. Protection accrue des données sensibles

Un régime plus protecteur doit être réservé aux données dites « sensibles », étant donné le risque plus élevé que leur traitement engendre pour la personne concernée. Le traitement de ces données sensibles n'est autorisé, selon la Convention 108+, qu'à la condition que des garanties appropriées supplémentaires, de nature à prévenir les risques pour les intérêts, droits et libertés fondamentales de la personne concernée, notamment un risque de discrimination, soient prévues par la loi.[106]

Le RGPD, quant à lui, renforce la protection accordée en présence de données sensibles en proclamant une interdiction de principe de tout traitement de telles données sauf exceptions prévues dans la liste restreinte de l'article 9.2. et à l'article 10.

Le choix fait par le législateur fédéral suisse s'inscrit dans la ligne de la Convention 108+ qui n'est pas d'interdire par principe le traitement des données sensibles, mais de l'encadrer de garanties supplémentaires. Ainsi, à titre d'exemple, la LPD prévoit qu'en cas de traitement de telles données avec le consentement de la personne concernée, ce consentement doit être exprès.[107] Par ailleurs, le responsable du traitement ne peut s'appuyer sur la simple balance d'intérêts pour traiter des données sensibles en vue d'évaluer la solvabilité de la personne concernée.[108] Il doit recourir au consentement dans ce cas.[109] En outre, une analyse d'impact préalable est requise en cas de traitement de données sensibles à grande échelle.[110] Quant aux traitements de données dans le secteur public fédéral, ils ne peuvent porter sur des données sensibles que s'ils s'appuient sur une base légale formelle.[111] Si des garanties additionnelles sont donc prévues par la LPD, on notera que cela ne couvre pas toutes les hypothèses de traitement de données sensibles, contrairement à ce qui est prévu dans les deux textes européens.

La liste des données qui sont considérées comme sensibles par la Convention 108+ figure à son article 6.1.[112] Cette catégorie particulière de données comprend tout d'abord les données sensibles par nature, présentant en toutes circonstances un caractère sensible : il s'agit des données génétiques et des données à caractère personnel concernant des infractions pénales (y compris présumées), des procédures et des condamnations pénales et des mesures de sûreté connexes. Ensuite sont considérées comme sensibles les données biométriques lorsqu'elles sont traitées aux fins d'identifier une personne physique de manière unique. Enfin, relèvent aussi de cette catégorie particulière les données sensibles par l'usage qui en est fait : les données à caractère personnel pour les informations qu'elles révèlent

106 Article 6 Convention 108+.
107 Article 6.7.a. LPD.
108 Article 31.2.c.1. LPD.
109 *Métille* (note 48), 5.
110 Article 22.2.a.LPD.
111 Article 34.2.a. LPD.
112 Pour le RGPD, cf. les articles 9 et 10.

sur l'origine raciale ou ethnique, les opinions politiques, l'appartenance syndicale, les convictions religieuses ou autres convictions, la santé ou la vie sexuelle.[113]

Les données de la dernière catégorie ne doivent être considérées comme sensibles que dans les cas où c'est précisément l'élément informationnel sensible contenu dans la donnée qui est traité. Ainsi, lorsque le traitement d'images enregistrées vise à révéler des informations sur l'origine raciale ou ethnique, ou sur la santé des personnes filmées, il s'agit d'un traitement de données sensibles. Alors qu'il s'agira d'un traitement de données ordinaires si les individus sont seulement filmés dans un contexte de vidéosurveillance à des fins de sécurité, sans chercher à traiter l'élément sensible figurant sur les images.[114]

La LPD présente à son article 5 let. c une liste de données personnelles sensibles très proche de la liste de textes européens puisqu'au sens de cette disposition on entend par données sensibles les données sur les opinions ou les activités religieuses, philosophiques, politiques ou syndicales, les données sur la santé, la sphère intime ou l'origine raciale ou ethnique, les données génétiques, les données biométriques identifiant une personne physique de manière univoque, les données sur des poursuites ou sanctions pénales et administratives et les données sur des mesures d'aide sociale. Deux types de données sont reconnus comme sensibles en Suisse alors qu'ils ne le sont pas dans la Convention 108+ ni dans le RGPD : il s'agit des données qui touchent à la sphère intime des individus (seule la vie sexuelle, relevant assurément de la sphère intime, est visée comme sensible par les textes européens) et celles sur les mesures d'aide sociale.

H. Obligations des acteurs

I. Sécurité des données

1. Mesures de sécurité appropriées

L'obligation d'adopter des mesures de sécurité existait déjà dans le texte de 1981 de la Convention 108. Elle a été reprise dans la version modernisée de 2018 avec, au passage, une clarification de la responsabilité de la sécurité : elle revient au responsable du traitement ainsi qu'à son sous-traitant s'il est recouru aux services d'un sous-traitant.

Ces acteurs doivent, selon les termes de l'article 7.1 de la Convention 108+, « prend[re] des mesures de sécurité appropriées contre les risques tels que l'accès accidentel ou non autorisé aux données à caractère personnel, leur destruction, perte, utilisation, modification ou divulgation ». Les mesures de sécurité à prendre

[113] Les données génétiques et biométriques sont nouvelles dans la liste des données sensibles par rapport à la liste de 1981. Les données relatives aux condamnations pénales ont été élargies aux infractions, procédures et mesures de sûreté. Quant aux autres données, elles figuraient déjà dans la liste initiale sauf les données révélant l'appartenance syndicale.

[114] Paragraphe 59 Rapport explicatif de la Convention 108+.

sont de deux ordres :[115] des mesures organisationnelles (limiter le nombre de personnes ayant accès aux données, utiliser des mots de passe renouvelés régulièrement, fermer les locaux où sont localisés les ordinateurs, etc.) et des mesures techniques (programme anti-virus fréquemment mis à jour, *firewalls, backup* de sécurité, *login*, etc.). Si le texte se contente de dire qu'il doit s'agir de mesures de sécurité « appropriées », le Rapport explicatif spécifie que le choix des mesures de sécurité doit tenir compte « des éventuels effets dommageables pour l'individu, de la nature des données à caractère personnel, du volume de données à caractère personnel traitées, du degré de vulnérabilité de l'architecture technique utilisée pour la réalisation du traitement, de la nécessité de restreindre l'accès aux données, des impératifs d'une conservation à long terme, etc. »[116] L'exigence de sécurité est donc modalisable en fonction des risques que le traitement fait courir aux personnes concernées.

A l'article 5.1.f. du RGPD, sous l'intitulé trompeur d'« intégrité et confidentialité », le devoir de sécurité des données figure au rang des principes de base de la protection des données dans le texte de l'Union européenne. Les données à caractère personnel doivent être traitées de façon à leur garantir une sécurité appropriée, ce qui inclut la protection contre le traitement non autorisé ou illicite et contre la perte, la destruction ou les dégâts d'origine accidentelle.[117] Le RGPD précise lui aussi que cette protection implique de prendre les mesures techniques ou organisationnelles appropriées.[118] Une section entière du chapitre dédié aux responsable et sous-traitant[119] développe ce devoir de sécurité.

Si une obligation de sécurité des données est présente dans la LPD depuis 1992, la nouvelle version de la loi a repris cette obligation au titre des dispositions générales (à son article 8) en apportant quelques précisions dans son énoncé. Ainsi, il est clarifié, dans la ligne des textes européens, que c'est à la fois sur les responsables du traitement et les sous-traitants que pèse le devoir d'assurer la sécurité des données. Par ailleurs, la sécurité doit désormais être « adéquate » par rapport au risque encouru.[120]

Au-delà de ces précisions, c'est surtout le paragraphe 2 qui introduit une grande nouveauté dans la loi suisse. Aux termes de ce paragraphe, « [l]es mesures doivent permettre d'éviter toute violation de la sécurité des données ».

2. Les violations de sécurité

La nouveauté en matière de sécurité se situe à l'article 7.2 de la Convention 108+ et aux articles 33 et 34 du RGPD qui tous instaurent une obligation de notifier à l'autorité de contrôle, voire aux personnes concernées, les atteintes à la sécurité,

115 Paragraphe 62 Rapport explicatif de la Convention 108+.
116 *Ibidem*.
117 Article 5.1.f. RGPD.
118 *Ibidem*.
119 Section 2 du chapitre IV consacré aux devoirs des responsable et sous-traitant, articles 32 à 34 RGPD.
120 *Sylvain Métille* y voit avec pertinence la matérialisation de l'approche de la protection des données fondée sur les risques ; cf. *Métille* (note 48), 12.

soit les violations de données, d'un certain niveau de gravité. Malgré la mise en place de mesures de sécurité, aucun responsable de traitement ou sous-traitant n'est en effet à l'abri d'une perte de données (surtout sur des supports mobiles ou portables) ou d'une faille de sécurité, les *hackers* faisant sans cesse preuve d'inventivité pour pénétrer les systèmes informatiques.

Le RGPD fournit une définition de ces violations de données qui doivent s'entendre de toute « violation de la sécurité entrainant, de manière accidentelle ou illicite, la destruction, la perte, l'altération, la divulgation non autorisée de données à caractère personnel transmises, conservées ou traitées d'une autre manière, ou l'accès non autorisé à de telles données ».[121] Cette définition sera reprise presqu'à l'identique dans la LPD.[122]

Le responsable du traitement doit notifier la violation de données sans délai excessif,[123] le RGPD précisant « dans les meilleurs délais et, si possible, 72 heures au plus tard après en avoir pris connaissance ».[124] Seules les violations susceptibles de porter gravement atteinte (selon la Convention 108+) ou d'engendrer un risque (selon le RGPD) pour les droits et libertés des personnes concernées doivent être notifiées par le responsable du traitement à l'autorité de contrôle. A titre d'exemples d'atteinte « grave » aux droits et libertés fondamentales des personnes concernées, le Rapport explicatif de la Convention 108+ cite la révélation de données couvertes par le secret professionnel, ou de données susceptibles d'entraîner un préjudice financier (comme les données liées à une carte de crédit) ou de causer une atteinte à la réputation, des dommages corporels ou une humiliation.[125]

Les textes européens font donc reposer sur le responsable du traitement la délicate question de savoir si une violation de données est susceptible de porter une atteinte grave ou de présenter un risque pour les droits et libertés des individus,[126] évaluation qui pourra *a posteriori* faire l'objet d'un contrôle de la part de l'autorité de protection des données.[127]

Selon le Rapport explicatif de la Convention 108+, signaler les violations de données aux autorités de contrôle est l'exigence minimale. Il faudrait également que le responsable du traitement soit tenu d'informer les autorités de contrôle des

121 Art. 4.12 RGPD.

122 La LPD définit à son article 5.h la violation de la sécurité des données comme étant « toute violation de la sécurité entraînant de manière accidentelle ou illicite la perte de données personnelles, leur modification, leur effacement ou leur destruction, leur divulgation ou un accès non autorisés à ces données ».

123 Article 7.2. Convention 108+.

124 Art. 33.1. RGPD.

125 Paragraphe 64 Rapport explicatif de la Convention 108+. Cf. également les exemples mentionnés dans Groupe de l'Article 29, Guidelines on Personal data breach notification under Regulation 2016/679, WP 250 révisées le 6 février 2018.

126 Sur la manière d'évaluer le risque engendré par une violation, cf. *Franck Dumotier*, Titre 4, La sécurité des traitements de données, les analyses d'impact et les violations de données, in : de Terwangne/Rosier (éd.), Le Règlement Général de Protection des données (RGPD/GDPR), Analyse approfondie, 2018, 243 ss.

127 *de Terwangne/Rosier/Losdyck* (note 36), n° 57.

mesures prises ou envisagées pour remédier à la violation et pallier les conséquences potentielles.[128] En outre, il peut être nécessaire d'informer les personnes concernées elles-mêmes, notamment lorsque la violation des données est de nature à engendrer un risque important pour leurs droits et libertés, « par exemple un traitement discriminatoire, un vol ou une usurpation d'identité, des pertes financières, une atteinte à la réputation, une perte de confidentialité des données protégées par le secret professionnel ou tout autre préjudice économique ou social lourd ».[129] Il conviendrait dans ce cas de renseigner les sujets des données sur les mesures à prendre pour atténuer les effets néfastes de la violation de leurs données.[130]

Pour le RGPD, la violation de données devra également être communiquée dans les meilleurs délais aux individus concernés si elle engendre un risque élevé pour leurs droits et libertés, à moins que le responsable du traitement ait appliqué aux données affectées des mesures de protection appropriées, en particulier des mesures qui rendent les données à caractère personnel incompréhensibles (par exemple grâce à la cryptographie), ou que le risque élevé ait été maitrisé par le responsable du traitement.[131] Toutefois, si une telle communication devait demander des efforts disproportionnés, le responsable du traitement pourrait procéder à une communication publique ou recourir à tout autre moyen permettant d'informer les personnes concernées.[132]

Par ailleurs, si le sous-traitant n'a pas l'obligation de notifier une violation de données à l'autorité de contrôle contrairement au responsable du traitement, il doit néanmoins notifier les violations de données dont il est victime au responsable du traitement dans les meilleurs délais.[133] Le responsable du traitement doit donc veiller à ce que ses sous-traitants lui transmettent les documents détaillant les violations de données qu'ils ont subies. En effet, une obligation de documentation de chaque violation de données pèse sur le responsable du traitement.

Cette nouvelle obligation d'annonce des violations de la sécurité des données se retrouve à l'article 24 de la LPD. En vertu de cette disposition, tout responsable du traitement, qu'il relève du secteur public ou du secteur privé, doit annoncer dans les meilleurs délais au PFPDT les atteintes à la sécurité des données entraînant vraisemblablement un risque élevé d'effets négatifs pour la personnalité ou les droits fondamentaux de la personne concernée. « Seuls les cas d'atteinte à la vie privée ou aux droits fondamentaux doivent être signalés au PFPDT, et non les cyberattaques déjouées avec succès ou inefficaces. »[134] Le seuil de l'obligation de déclaration correspond à celui retenu par la Convention 108+ mais est plus haut que celui du RGPD qui déclenche l'obligation d'information dès que la violation des données comporte un risque pour les personnes concernées.

128 Paragraphe 65 Rapport explicatif de la Convention 108+.
129 Paragraphe 66 Rapport explicatif de la Convention 108+.
130 *Ibidem*.
131 Art. 34.1. RGPD.
132 Art. 34.3.c RGPD.
133 Art. 33.2 RGPD.
134 PFPDT (note 7), 6.

La LPD prévoit également un devoir d'information à l'égard de la personne concernée « lorsque cela est nécessaire à sa protection »[135] – formule assurément plus souple cette fois que celle du « risque élevé pour les droits et libertés » du RGPD – ou lorsque le PFPDT l'exige.[136] Le responsable du traitement peut toutefois renoncer à alerter les personnes concernées de la violation de leurs données lorsque cela mettrait à mal des intérêts publics ou privés prépondérants ou nécessiterait des efforts disproportionnés. Comme le RGPD, la LPD[137] permet l'information par la voie d'une communication publique si le résultat est équivalent à celui obtenu par la voie individuelle.

II. Transparence du traitement de données

Tant la Convention 108+[138] que le RGPD[139] prévoient que le responsable du traitement est tenu de communiquer spontanément une série d'informations aux personnes concernées par les données qu'il traite. Il s'agit d'indiquer son identité et ses coordonnées (le RGPD ajoutant celles de son représentant si le responsable est établi hors de l'Union européenne et celles de l'éventuel délégué à la protection des données), la base légale (si le traitement se fonde sur une balance d'intérêts – article 6.1.f. RGPD – le RGPD demande en outre de mentionner les intérêts légitimes liés à ce traitement) et les finalités du traitement, les catégories de données traitées et leurs destinataires ainsi que les moyens d'exercer les droits.

D'autres informations doivent être également transmises aux personnes concernées lorsque c'est nécessaire pour garantir un traitement loyal et licite, parmi lesquelles figurent notamment la durée de conservation des données ou l'information sur les pays tiers vers lesquels les données seront communiquées si elles sont destinées à partir vers l'étranger.

Le RGPD ajoute encore une information particulièrement importante dans nos sociétés imprégnées d'automatisation et en quête d'explicabilité des décisions prises par des algorithmes : il faut signaler l'existence d'une décision automatisée ou d'un profilage, et fournir des informations sur la logique sous-jacente et sur les conséquences découlant de cette décision automatisée ou de ce profilage pour la personne concernée.[140]

Ce devoir d'information s'impose, que la collecte des données s'effectue directement auprès de la personne concernée ou indirectement, auprès d'un tiers ou d'une autre source.[141]

L'article 14.4 du RGPD ajoute encore un nouvel élément au cas où le responsable du traitement aurait l'intention d'effectuer un traitement ultérieur des don-

135 Article 24.4 LPD.
136 *Ibidem*.
137 Article 24.5 LPD.
138 Article 8 Convention 108+.
139 Articles 13 et 14 RGPD.
140 Articles 13.2 et 14.2 RGPD.
141 Article 14.1.d RGPD.

nées à caractère personnel pour une finalité autre que celle pour laquelle les données à caractère personnel ont été obtenues. Dans ce cas, ce responsable doit fournir, au préalable, des informations au sujet de cette autre finalité à la personne concernée. En particulier, il doit indiquer en quoi le traitement ultérieur est à ses yeux compatible avec la finalité du traitement originaire.[142]

L'ensemble de ces informations, qui doivent être facilement accessibles et compréhensibles, peuvent être fournies sous tout format approprié (par le biais d'un site web, d'outils technologiques sur des appareils personnels, etc.) pourvu qu'elles soient présentées de manière effective et loyale à la personne concernée.[143]

Le droit à l'information n'est bien sûr pas absolu et une série d'exceptions peuvent intervenir.

L'article 19 de la LPD impose au responsable du traitement une obligation d'information inspirée de (mais non identique à) celle prévue dans la Convention 108+, c'est-à-dire un peu moins développée que celle du RGPD. Le paragraphe 2 de l'article 19 éclaire utilement le but de cette obligation : il s'agit de permettre à la personne concernée de faire valoir ses droits et de garantir la transparence des traitements.

III. Obligations complémentaires

L'article 10 de la Convention 108+ ajoute aux obligations de transparence et de sécurité des obligations complémentaires. Ces obligations complémentaires se retrouvent dans le RGPD et, à part pour l'*accountability*, dans la LPD. Il s'agit de la mise en conformité (*accountability*) (1), de la désignation d'un délégué à la protection des données (2), de l'examen de l'impact du traitement (3), et de la prise en compte de la protection des données dès la conception et par défaut (4).[144]

1. La responsabilité de la conformité

Par l'application du principe d'*accountability*, le responsable du traitement et, le cas échéant, son sous-traitant, sont tenus de prendre toutes les mesures appropriées afin de se conformer aux règles de la protection des données et ils doivent être en mesure de démontrer à tout instant leur conformité avec ces règles.[145] Ils doivent donc mettre en place des mécanismes internes permettant de démontrer la conformité des traitements avec les dispositions applicables.

---

142 Groupe 29, Guidelines on transparency under Regulation 2016/679, WP 260, 12 décembre 2017, 20; *Thomas Tombal*, Titre 9, Les droits de la personne concernée dans le RGPD, in : de Terwangne/Rosier (éd.), Le Règlement Général de Protection des données (RGPD/GDPR), Analyse approfondie, 2018, 423.

143 Paragraphe 68 Rapport explicatif de la Convention 108+ ; article 12 RGPD.

144 Il est à noter que le RGPD exige en outre la tenue d'un registre interne des traitements réalisés (article 30 RGPD), obligation que l'on retrouve à l'article 12 LPD.

145 Article 10.1. Convention 108+; articles 5.2 et 24 RGPD. Sur le principe d'*accountability*, cf. Groupe de l'Article 29, Avis 3/2010 du 13 juillet 2010 sur le principe de la responsabilité, WP 173 ; *Antoine Delforge,* L'obligation générale d'« accountability », in: La protection des données à caractère personnel en Belgique, Manuel de base, 2019, 79 ss.

A titre d'exemples de mesures appropriées permettant aux responsables et aux sous-traitants de se mettre en conformité, le Rapport explicatif de la Convention 108+ cite « la formation des employés, la mise en place de procédures appropriées de notification (indiquant par exemple quand des données doivent être effacées du système), l'établissement de clauses contractuelles particulières en cas de délégation du traitement visant à donner effet à la Convention, ainsi que la mise en place de procédures internes permettant la vérification et la démonstration de la conformité. »[146]

2. La désignation d'un délégué à la protection des données

C'est aussi comme mesure destinée à faciliter la vérification et la démonstration de la conformité des traitements de données que les auteurs de la Convention 108+ proposent que le responsable de traitement désigne un délégué à la protection des données.[147] Le Rapport explicatif précise qu'il « pourra s'agir d'un agent interne ou externe au responsable du traitement et sa désignation devra être notifiée à l'autorité de contrôle ».[148]

Cette proposition a pris la forme d'une obligation expresse dans le RGPD.[149] Depuis l'avènement de ce règlement européen, ce nouveau venu qu'est le délégué à la protection des données (*data protection officer*, DPO) s'est vu recruté par milliers à travers l'Europe et le monde.[150] Sa désignation par le responsable du traitement ou par le sous-traitant est obligatoire ou optionnelle selon le cas.[151]

Le DPO doit informer et conseiller le responsable du traitement ou le sous-traitant qui l'a désigné et servir de point de contact avec l'autorité de contrôle ou les personnes concernées.[152] Le RGPD impose des garanties pour que le délégué puisse avoir une connaissance effective des activités de traitement et travailler de manière indépendante et sans crainte de se voir sanctionner pour les avis ou conseils qu'il donne.[153]

Quant à la LPD, elle prévoit elle aussi la fonction du « spécialiste maison » en matière de protection des données, qu'elle a baptisé conseiller à la protection des données. En vertu de son article 10, les entreprises peuvent choisir de nommer un conseiller à la protection des données qui peut être interne ou externe à l'entreprise. Des garanties d'indépendance doivent être données. Contrairement à ce que prévoit

146 Paragraphe 85 du Rapport explicatif de la Convention 108+.
147 Paragraphe 87 du Rapport explicatif de la Convention 108+.
148 *Ibidem*.
149 Article 37 RGPD.
150 Sur la notion et le rôle du DPO, cf. *Karen Rosier*, Délégué à la protection des données : une fonction multifacette, in : de Terwangne/Rosier (éd.), Le Règlement Général de Protection des données (RGPD/GDPR), Analyse approfondie, 2018, 559 ss.
151 Art. 37.1.a. Cf. Groupe de l'Article 29, Lignes directrices du 13 décembre 2016 révisées le 5 avril 2017, concernant les délégués à la protection des données (DPD), WP243, 8.
152 Art. 37.5 RGPD. Pour les fonctions du délégué, cf. l'art. 39, §1er du RGPD.
153 Art. 38, §§ 2 et 3 du RGPD. Pour une présentation détaillée, cf. *Delforge* (note 57), 90 ss.

le RGPD, la désignation de conseillers à la protection des données au sein du secteur privé est donc facultative alors qu'il s'agit d'une obligation légale pour les organes fédéraux.[154]

3. L'examen/analyse d'impact

La Convention 108+ prévoit qu'avant de se mettre à traiter des données à caractère personnel, le responsable du traitement a l'obligation de procéder à un examen de l'impact de ce traitement de données sur les droits et libertés fondamentales d'autrui.[155] Il doit ensuite concevoir le traitement de manière à minimiser cet impact. Lors de cet examen, le responsable du traitement est appelé à évaluer le respect du principe de proportionnalité à tous les stades envisagés du traitement de données et à aménager son traitement de façon à éviter les atteintes disproportionnées aux droits des personnes concernées.[156]

Le RGPD réserve l'obligation de procéder à une analyse des risques que présente le traitement envisagé sur les droits et libertés fondamentales d'autrui aux seuls cas où le traitement est susceptible d'engendrer un risque élevé pour ces droits et libertés.[157] Cette analyse appelée « analyse d'impact relative à la protection des données » (AIPD – ou *privacy impact assessment* (*PIA*)) vise à déterminer les mesures à prendre pour prévenir le ou les risques identifiés.[158]

D'après le PFPDT, cette démarche d'analyses préalables de l'impact des traitements de données n'est « pas une nouveauté dans le droit suisse de la protection des données – les organes fédéraux sont déjà tenus de les réaliser ».[159] L'art. 22 de la LPD l'impose désormais également pour les responsables de traitement du secteur privé dès qu'un traitement est susceptible d'entraîner un risque élevé pour la vie privée ou les droits fondamentaux des personnes concernées. Le risque élevé peut provenir de la nature, de la portée, du contexte ou des finalités du traitement, en particulier lors du recours à des technologies nouvelles.

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

La Convention 108+[160] tout comme le RGPD[161] exigent des responsables de traitement qu'ils intègrent la préoccupation de la protection des données au sein même des systèmes, produits et services créés, et cela, dès les premiers stades de leur conception. C'est le devoir de *privacy by design*. Les responsables doivent mettre en œuvre des mesures techniques et organisationnelles appropriées afin de répondre

154 *Métille* (note 48), 18.
155 Article 10.2 Convention 108+.
156 Paragraphe 88 du Rapport explicatif de la Convention 108+.
157 Art. 35 du RGPD. Cf. *Delforge* (note 57), 99 ss.
158 cf. EDPB, Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679, wp248rev.01, 13 octobre 2017.
159 PFPDT (note 7), 4.
160 Article 10.3 Convention 108+.
161 Article 25 RGPD.

à l'ensemble des exigences légales en matière de protection des données, notamment afin de permettre aux personnes concernées d'exercer efficacement leurs droits. Ainsi, un accès sécurisé aux données en ligne devrait être proposé aux personnes concernées chaque fois que possible. Il devrait également y avoir des outils faciles à utiliser permettant aux personnes concernées de transférer leurs données à un autre fournisseur de service (outils de portabilité des données – cf. *supra* I.VI.).[162]

Le RGPD a ajouté un devoir de *privacy by default*, c'est-à-dire d'organisation ou de paramétrage par défaut du traitement permettant de respecter le principe de minimisation des données et ne concourant pas au traitement de données non nécessaires pour atteindre la finalité voulue.

La LPD fait figurer cette double exigence à son article 7 qui demande dans un premier temps (7.1) de mettre en place, dès la conception du traitement, des mesures techniques et organisationnelles afin de respecter les prescrits légaux de protection des données ; et, dans un deuxième temps, (7.3) de garantir, par le biais de préréglages appropriés, que le traitement des données personnelles soit limité au minimum requis par la finalité poursuivie. La LPD permet toutefois qu'on puisse dépasser ce seuil minimum avec le consentement de la personne concernée.

I. Droits des personnes concernées

Des droits sont reconnus par le Conseil de l'Europe aux personnes concernées depuis 1981, tels que le droit d'accès aux données, le droit de les rectifier ou de les effacer et le droit de recours (art. 8, b, c et d de la Convention 108). Ces droits sont renforcés dans le texte modernisé de la Convention, tandis que de nouveaux droits sont venus compléter la liste (article 9 Convention 108+).

Le RGPD offre pour sa part le catalogue de droits le plus élaboré parmi les instruments juridiques de protection des données, dans la ligne des droits énumérés dans le nouvel article 9 de la Convention, mais sensiblement plus développés.

Ces droits sont présentés dans les paragraphes ci-dessous, en suivant l'ordre de l'article 9 de la Convention 108+. Le droit à l'information a été évoqué ci-dessus sous forme d'obligation de transparence (cf. *supra* H.II).

Tous ces droits ne sont pas absolus. Des exceptions sont admises pour chacun d'entre eux. Dans les deux textes européens,[163] une disposition est spécialement consacrée aux exceptions que les Parties ou Etats membres ont la possibilité d'adopter à l'égard des principales dispositions de la Convention et du RGPD, parmi lesquelles les dispositions relatives aux droits des personnes concernées. Pour être admises, ces exemptions doivent être prévues par la loi et constituer une mesure nécessaire dans une société démocratique pour la protection de certains intérêts publics ou privés.

[162] Paragraphe 89 Rapport explicatif de la Convention 108+.
[163] Article 11 Convention 108+ ; article 23 RGPD.

I. Droit de ne pas faire l'objet d'une décision individuelle automatisée

Le droit de ne pas être soumis à une décision entièrement automatisée découle de la conviction que les machines ne peuvent dominer les êtres humains. Il n'est pas souhaitable qu'une décision imposée à une personne dépende des seules conclusions d'une machine. En ce sens, l'article 9.1.a. de la Convention 108+ garantit à toute personne le droit « de ne pas faire l'objet d'une décision l'affectant de manière significative prise sur le seul fondement d'un traitement automatisé de données sans que son point de vue soit pris en considération ».

Ce droit était déjà présent dans la directive 95/46/CE[164] et est repris dans l'article 22 du RGPD qui énonce dans des termes assez similaires : « La personne concernée a le droit de ne pas faire l'objet d'une décision fondée exclusivement sur un traitement automatisé, y compris le profilage, produisant des effets juridiques la concernant ou l'affectant de manière significative de façon similaire. » Les décisions automatisées sont toutefois admises dans le cadre d'un processus contractuel ou avec le consentement de la personne concernée mais dans les deux cas, la personne concernée doit avoir le droit d'obtenir une intervention humaine de la part du responsable du traitement, d'exprimer son point de vue et de contester la décision.[165]

La LPD contient, elle aussi, une disposition préservant le droit de la personne concernée face à la machine. Intitulé « Devoir d'informer en cas de décision individuelle automatisée », l'article 21 LPD va en fait plus loin que se limiter à la question de l'information de la personne concernée. Une fois celle-ci dûment informée de toute décision prise exclusivement sur la base d'un traitement de données automatisé ayant des effets juridiques pour elle ou l'affectant de manière significative, la LPD lui reconnait le droit de demander à faire valoir son point de vue ou d'exiger que la décision individuelle automatisée soit revue par une personne physique. Il s'agit donc bien, au-delà de la simple information, du droit de remettre l'humain dans la boucle des décisions individuelles automatisées.

II. Droit d'accès enrichi

Les auteurs de la Convention 108+ et du RGPD ont étendu le droit d'accès de manière à intégrer davantage d'informations à communiquer à la personne concernée exerçant son droit. Ainsi, outre la communication sous une forme intelligible des données traitées[166] ou d'une copie des données faisant l'objet du traitement,[167] le droit d'accès implique l'accès aux finalités du traitement, aux destinataires des données, à la période de conservation, à l'origine des données, à l'existence d'une prise de décision automatisée ou d'un profilage et à des informations utiles concer-

164 Article 12.a directive 95/46.
165 Article 22.2.a et c et article 22.3 RGPD.
166 Article 9.1.b Convention 108+ ; Articles 12.1. et 15 RGPD.
167 Article 15.3 RGPD.

nant la logique sous-jacente, ainsi qu'aux garanties entourant les éventuels transferts de données vers l'étranger.[168] La personne concernée est aussi en droit d'obtenir des informations sur ses droits de rectification, d'effacement et de recours, droits qu'elle voudra peut-être mobiliser une fois qu'elle aura découvert le sort de ses données grâce au droit d'accès.

L'article 25 de la LPD offre aux personnes concernées un droit d'accès enrichi dans la même mesure. Au-delà de la liste des informations que la personne concernée peut obtenir, correspondant à celle du RGPD, d'autres informations pourraient même lui être communiquées si elles s'avèrent nécessaires pour qu'elle « puisse faire valoir ses droits [...] et pour que la transparence du traitement soit garantie ».[169]

Il est à noter que la loi suisse prévoit des limitations au droit d'accès qui vont plus loin que celles admises par les textes européens. Ceux-ci permettent aux Parties ou Etats membres de prévoir des exceptions aux droits, notamment si c'est nécessaire pour garantir la protection des droits et libertés d'autrui.[170] Or, l'article 26 de la LPD permet de refuser l'accès quand les intérêts prépondérants d'un tiers (article 26.1.b) ou de la personne privée responsable du traitement l'exigent et, dans ce dernier cas, que les données ne soient pas communiquées à un tiers (article 26.2.a). La notion d'intérêt prépondérant est plus large que celle de droit et liberté et pourrait englober un intérêt économique (une entreprise pourrait être tentée de rejeter une demande d'accès parce que cela induirait un travail fastidieux et coûteux pour elle) ou tout autre intérêt (une entreprise ne veut pas donner accès aux évaluations internes de son personnel car elle craint que les évaluateurs ne s'expriment plus librement si leurs commentaires sont transmis aux intéressés). Par ailleurs, l'article 26.1.c LPD permet de refuser les demandes d'accès lorsqu'elles sont manifestement infondées, notamment parce qu'elles poursuivent un but contraire à la protection des données. Le législateur suisse a voulu freiner l'instrumentalisation de la protection des données au service d'un autre objectif. Or, au-delà du fait qu'elle n'est pas prévue par les textes européens, pareille exception est contraire à l'esprit-même du droit d'accès car elle revient à permettre d'exiger de la personne concernée qu'elle motive sa demande d'accès.

III. Droit de connaître le raisonnement qui sous-tend le traitement des données

Dans le contexte technologique actuel, il existe un droit de grand intérêt, notamment face au phénomène exponentiel du profilage où l'on se base sur des profils pour prendre des décisions sur une personne ou prédire ses préférences, son comportement et ses attitudes personnelles. Il s'agit du droit de connaître le raisonnement qui sous-tend un traitement de données dont les résultats sont appliqués à un individu. Face à un refus de crédit, un échec à un examen à questions à choix multiples, un ciblage comme fraudeur présumé, etc., il est clair que l'on peut vouloir

168 Article 9.1.b Convention 108+; Article 15.1.a,c,d,g RGPD.
169 Article 25.2 LPD ; *Métille* (note 48), 31.
170 Article 11.1.b Convention 108+ et article 23.1.i RGPD.

comprendre l'évaluation ou la décision en accédant au raisonnement qui sous-tend le traitement des données. On peut légitimement vouloir connaître les critères utilisés et le poids accordé à chacun de ces critères.

Ce droit est un droit clé qui contribue largement à la transparence et donc à l'autodétermination informationnelle des individus car il leur permet non seulement de **savoir** ce qui se passe avec leurs données, mais aussi de **comprendre**.

Ce droit a été garanti pour la première fois par la directive 95/46.[171] Il a logiquement été repris dans le RGPD.[172] Comme exposé dans ce dernier texte, le droit de recevoir des informations ainsi que le droit d'accès comprennent le droit de connaître l'existence d'une prise de décision automatisée, y compris le profilage, et, au moins dans ces cas, de recevoir des informations significatives sur la logique impliquée, ainsi que l'importance et les conséquences prévisibles de ce traitement pour la personne concernée.

Quant aux auteurs de la Convention 108+, ils ont ajouté à la liste des garanties offertes aux personnes concernées le droit pour toute personne d'« obtenir, sur demande, la connaissance des motifs qui sous-tendent le traitement des données lorsque les résultats de ce traitement lui sont appliqués ».[173]

Les auteurs de la LPD, eux aussi, ainsi qu'on l'a vu au point ci-dessus, ont prévu le droit à cette information concernant la logique sur laquelle se base la décision individuelle automatisée.

IV. Droit d'opposition

Les deux textes européens[174] prévoient un droit d'opposition au traitement de données. Les personnes ont le droit de s'opposer à tout moment, pour des raisons tenant à leur situation, au traitement de données à caractère personnel les concernant, à moins que le responsable du traitement ne démontre des motifs légitimes pour poursuivre le traitement qui prévalent sur les intérêts ou les droits et libertés fondamentales de la personne concernée.

Ce droit est particulièrement approprié lorsque le traitement des données n'est pas fondé sur le consentement de la personne concernée. Il est important dans les cas où le responsable du traitement a lui-même mis en balance les intérêts en jeu au préalable et a conclu que le résultat est équilibré et qu'il pouvait légitimement traiter les données.[175] Grâce au droit d'opposition, la personne concernée a la possibilité de contester le résultat de cette mise en balance, du moins dans son cas personnel.

La charge de la preuve incombe au responsable du traitement qui doit démontrer que ses intérêts légitimes à traiter les données prévalent sur les droits et intérêts de

171 Article 12.a Directive 95/46.
172 Articles 13.2.f, 14.2.g et 15.1.h RGPD.
173 Article 9.1.c. Convention 108+.
174 Article 9.1.d Convention 108+; article 21 RGPD.
175 Article 6.1.f RGPD.

la personne concernée. Comme il est pleinement informé du traitement qu'il effectue sur les données, il semble mieux placé que la personne concernée pour argumenter sur la balance des intérêts en jeu.

La LPD prévoit un droit d'opposition dans plusieurs cas :

- La personne concernée a le droit de s'opposer à ce qu'un organe fédéral communique ses données personnelles, à condition de rendre vraisemblable un intérêt digne de protection empêchant la communication (article 37.1 LPD) ;
- En cas de traitement par une personne privée, le droit d'opposition découle du fait que traiter des données personnelles contre la manifestation expresse de la volonté de la personne concernée constitue une atteinte à la personnalité (article 30.2.b).[176] Cette atteinte sera jugée comme illicite sauf si la poursuite du traitement malgré la manifestation de la volonté de la personne concernée est justifiée par un intérêt privé ou public prépondérant, ou par la loi (article 31.1) ;[177]
- Le cas très particulier où la personne concernée peut s'opposer à la réutilisation de ses données qu'elle avait elle-même rendues publiquement accessibles (article 30.3 et 36.2.d LPD).

D'après *Sylvain Métille*, le droit d'opposition se déduit aussi du droit à l'autodétermination informationnelle basé sur l'article 13 de la Constitution.[178]

V. Droit de rectification et d'effacement – droit à l'oubli

Le droit d'obtenir la rectification des données inexactes et l'effacement des données qui ont été traitées en violation des règles de protection des données est accordé aux personnes concernées depuis l'adoption du tout premier texte européen.[179] Ce droit n'a pas changé et est protégé par la Convention 108+[180] ainsi que par le RGPD.[181]

Dans le RGPD, le droit à l'effacement est présenté comme étant associé au « droit à l'oubli ». Dans l'environnement Internet, ce droit est apparu comme une réponse appropriée aux problèmes soulevés par la mémoire électronique éternelle (créant l'« effet d'éternité ») combinée au pouvoir d'extraction et de rassemblement des moteurs de recherche (et la décontextualisation des données qui en résulte). Comme les autres droits, ce droit à l'effacement/à l'oubli n'est pas absolu

176 Rapport explicatif de la commission des affaires juridiques du Conseil national du 28 octobre 2002, FF 2003 1921, 1925, « Le droit de la personne concernée de s'opposer à ce que des personnes privées traitent des données personnelles la concernant, est réglée à l'art. 12, al. 2, let .b, LPD [équivalant à l'article 30.2.b de la loi nouvelle LPD] ». Dans le même sens *Métille* (note 48), 33.

177 « Il découle de cette disposition que la personne concernée a le droit d'interdire explicitement un certain traitement, sans avoir à remplir d'autres conditions (opting out). » ; cf. Département fédéral de justice et police, Rapport explicatif concernant l'avant-projet de loi fédérale sur la révision totale de la loi sur la protection des données et sur la modification d'autres lois fédérales, 2016, 65.

178 *Ibidem*.

179 Article 8.c Convention 108.

180 Article 9.1.e Convention 108+.

181 Articles 16 et 17 RGPD.

et des limitations sont admises mais, contrairement aux autres droits, ces limitations ne sont pas laissées au choix des États membres : elles sont inscrites dans l'article 17 du RGPD lui-même.

La LPD garantit le droit à la rectification et à l'effacement ou la destruction des données à ses articles 32 et 41. Il est à noter que, dans les cas de traitements effectués par un organe fédéral, l'exercice du droit de rectification et d'effacement peut conduire à une mise en balance du droit de la personne concernée à voir ses données corrigées ou effacées avec les intérêts publics ou de tiers (article 41.3).

S'il ne peut être procédé à la rectification ou l'effacement des données parce que l'exactitude des données ne peut être établie ou parce qu'un intérêt public ou l'intérêt d'un tiers prépondérants l'exigent, le caractère litigieux de la donnée est ajouté à celle-ci. Un devoir de limitation[182] de l'utilisation des données contestées pèse alors sur l'organe public concerné.

La LPD prévoit un droit de suite : la personne concernée peut demander que la décision de rectification, d'effacement ou de destruction des données, ou la mention du caractère litigieux des données en cause soient publiées ou communiquées à des tiers. Un tel droit de suite est prévu par le RGPD[183] et est mentionné dans le Rapport explicatif de la Convention 108[184] (paragraphe 81). Mais plutôt qu'un droit qui n'est activé qu'à la demande de la personne concernée, il s'agit dans les textes européens d'une obligation automatique.[185]

VI. Droit à la portabilité des données

L'article 20 du RGPD a créé un nouveau droit à la portabilité des données qui permet aux personnes concernées de recevoir les données personnelles qu'elles ont fournies à un responsable du traitement, dans un format structuré, couramment utilisé et lisible par machine, afin de transmettre ces données à un autre responsable du traitement.[186] Lorsque cela est techniquement possible, le responsable du traite-

182 Correspondant à l'article 18 du RGPD qui instaure un droit à la limitation du traitement des données en cas de contestation.

183 Article 19 RGPD: Le responsable du traitement notifie à chaque destinataire auquel les données à caractère personnel ont été communiquées toute rectification ou tout effacement de données à caractère personnel ou toute limitation du traitement effectué conformément à l'article 16, à l'article 17, paragraphe 1, et à l'article 18, à moins qu'une telle communication se révèle impossible ou exige des efforts disproportionnés. Le responsable du traitement fournit à la personne concernée des informations sur ces destinataires si celle-ci en fait la demande.

184 Paragraphe 81: Lorsque des rectifications et des effacements sont obtenus conformément au principe énoncé à l'alinéa *e*, ils doivent, dans la mesure du possible, être portés à la connaissance des destinataires de l'information originale, à moins que cela se révèle impossible ou implique des efforts disproportionnés.

185 L'intitulé de l'article 19 RGPD est d'ailleurs « *Obligation* de notification en ce qui concerne la rectification ou l'effacement de données à caractère personnel ou la limitation du traitement ».

186 Article 20 RGPD. Cf. Article 29 Data Protection Working Party, Guidelines on the right to data portability, 13 décembre 2016, last revised and adopted on 5 April 2017 WP 242 rev.01, 3.

ment doit transmettre les données lui-même, à la demande de la personne concernée, directement à un autre responsable du traitement.[187] L'objectif de ce nouveau droit est de responsabiliser la personne concernée et de lui donner plus de contrôle sur les données personnelles qui la concernent.[188] En permettant aux personnes concernées de transférer facilement leurs données d'un environnement numérique à un autre, sans entrave, la portabilité des données donne aux consommateurs les moyens d'agir et empêche le verrouillage des données.[189]

C'est à l'article 28 que la LPD prévoit, de la même manière que le RGPD, le droit à la portabilité des données, baptisé « droit à la remise ou à la transmission des données personnelles ».

J. Flux transfrontières de données/Communication de données à l'étranger

Pour déterminer le champ de la question des flux transfrontières de données, l'Exposé des motifs de la Convention 108+ indique : « Un transfert transfrontière de données intervient lorsque des données à caractère personnel sont communiquées ou mises à disposition d'un destinataire relevant de la juridiction d'un autre État ou d'une autre organisation internationale. »[190] Pour le RGPD, c'est dans un texte adopté par le Comité européen de la protection des données (EDPB) que l'on trouve une définition du transfert de données à l'étranger. Ainsi, on est en présence d'un tel transfert de données «when [data] travels to third countries »[191] mais aussi « remote access from a third country (for example in support situations) and/or storage in a cloud situated outside the EEA offered by a service provider, is also considered to be a transfer ».[192] La notion de transfert recouvre donc, dans les deux textes, aussi bien l'envoi de données au-delà des frontières que la mise à disposition des données permettant leur accès depuis un Etat tiers.

La LPD, quant à elle, recourt à la notion de communication qu'elle définit comme « le fait de transmettre des données personnelles ou de les rendre accessibles » (article 5.e. LPD). Cette définition correspond donc à celle de l'Exposé des motifs de la Convention 108+. Toutefois, l'article 18 de la loi apporte la précision que la publication de données personnelles au moyen de services d'information et de communication automatisés afin d'informer le public n'est pas assimilée à une communication à l'étranger, même si ces données peuvent être consultées depuis l'étranger. La diffusion de données via Internet n'est donc pas considérée comme une communication et, dès lors, le régime des communications à l'étranger ne s'applique pas dans le cas d'une telle diffusion. Or, cela signifie que

187 Article. 20.2 RGPD.
188 cf. Article 29 Data Protection Working Party (note 186), 3 s.
189 *Ibidem*.
190 Paragraphe 102 Rapport explicatif de la Convention 108+.
191 EDPB, Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, version 2.0 adopted on 18 June 2021, pt 2.
192 *Ibidem*, pt 13.

la publication sur Internet n'est pas soumise à la protection accrue réservée aux communications de données vers l'étranger. Il est dommage qu'une voie de mise à disposition de données qui permet très facilement aujourd'hui des transferts de données dès que des personnes téléchargent depuis l'étranger les données publiées sur les sites Internet, ne soit pas soumise au régime protecteur plus exigeant. Des données personnelles se retrouvent par cette voie dénuées de protection adéquate, sous des cieux lointains où il peut s'avérer extrêmement difficile d'exercer ses droits.

Le régime des flux transfrontières de données est organisé dans la Convention 108+ en distinguant les flux de données personnelles vers d'autres Parties à la Convention et ceux vers des non-Parties. Entre les Parties, la règle reste celle de la libre circulation, sauf si la Partie expéditrice est «liée par des règles de protection harmonisées communes aux États membres d'une organisation internationale régionale».[193] Dans ce cas, un transfert de données peut néanmoins avoir lieu s'il est régi par des mesures ad hoc ou standardisées. La liberté des flux n'est donc pas systématique entre les Parties à la Convention 108+. Cela s'explique par la nécessité de coordonner les deux sphères juridiques européennes et de prendre en compte les contraintes issues du régime juridique de l'Union européenne.

Les transferts vers des destinataires ne relevant pas de la juridiction d'une Partie à la Convention ne peuvent avoir lieu que si un niveau approprié de protection des données fondé sur les principes de la Convention est garanti.[194] Ce niveau approprié de protection peut être assuré par le droit de cet État ou de cette organisation internationale, y compris les traités ou accords internationaux applicables. Si aucune loi n'offre une protection appropriée, celle-ci peut être garantie par plusieurs mécanismes. Elle peut être assurée par des garanties ad hoc ou standardisées,[195] comme des clauses contractuelles ou des règles d'entreprise contraignantes.

Quant au RGPD,[196] il ne change pas grand-chose au régime de la directive 95/46 de 1995 mais il apporte des précisions nouvelles à propos des conditions pour reconnaitre un niveau de protection adéquat et il élargit la liste des instruments juridiques qui peuvent être utilisés pour prévoir des garanties appropriées et ainsi permettre les transferts transfrontières de données (clauses contractuelles, règles d'entreprise contraignantes, arrangements administratifs entre autorités ou organismes publics, codes de conduite et mécanismes de normalisation).

La LPD[197] encadre les transferts de données vers l'étranger des mêmes garanties que celles présentes dans les textes européens. Une nuance apparait concernant l'information à transmettre systématiquement (pour la Convention 108+[198]) ou seulement sur demande (pour la LPD[199]) à l'autorité de contrôle à propos de l'utilisation de garanties ad hoc pour entourer des transferts de données.

193 Article 14.1 Convention 108+.
194 Article 14.2 Convention 108+.
195 Article 14.3 Convention 108+.
196 Chapitre V RGPD.
197 Article 16 et 17 LPD.
198 Article 14.5 LPD.
199 Article 17.2 LPD.

K. Les autorités de contrôle

Les autorités de contrôle spécialisées font partie intégrante du système européen de protection des données à caractère personnel.[200] Sur l'ensemble du territoire européen, les autorités de contrôle nationales sont chargées de veiller au respect de toutes les règles de protection des données décrites dans les pages précédentes.

Tant la Convention 108+ que le RGPD instituent des autorités de protection des données (APD),[201] veillent à l'indépendance de ces autorités[202] et à leur dialogue, leur coopération et leur assistance mutuelle.[203]

Les autorités nationales de protection des données ont pour mission de mettre en œuvre et faire respecter les règles de protection des données. Elles contrôlent, par des pouvoirs d'investigation et d'intervention, l'application des règles de protection des données.[204] Elles traitent les plaintes déposées pour violation de ces règles.[205] En outre, elles fournissent des conseils d'experts sur les questions de protection des données.[206] Un changement majeur dans les nouveaux textes européens réside dans l'octroi aux APD de pouvoirs de décision et de sanction importants,[207] y compris la capacité d'imposer des amendes substantielles aux responsables du traitement et aux sous-traitants en vue d'une meilleure application des règles. Le Rapport explicatif de la Convention 108+ précise que « lorsque le système juridique de la Partie ne prévoit pas l'imposition de sanctions administratives, le paragraphe 2 peut être appliqué de sorte à ce que la sanction soit proposée par l'autorité de contrôle compétente et prononcée par l'autorité judiciaire compétente ».[208] Selon le RGPD, les amendes administratives peuvent aller jusqu'à 20 millions d'euros ou, dans le cas d'une entreprise, 4% du chiffre d'affaires annuel mondial.[209]

En Suisse, l'autorité de contrôle fédérale, le PFPDT, est chargée de surveiller la bonne application des dispositions fédérales de protection des données.[210] Le préposé dispose désormais d'un pouvoir d'enquête[211] et d'un véritable pouvoir de décision autonome[212] à l'encontre des organes fédéraux et des responsables de traitement privés. Il peut ordonner des mesures administratives telles qu'adapter le traitement des données problématique, le suspendre, le faire cesser, et faire effacer ou détruire les données personnelles litigieuses. Mais il n'a pas reçu le pouvoir d'infliger lui-même des amendes administratives ni pénales en cas d'infraction à la LPD. Il peut toutefois dénoncer des infractions aux autorités de poursuite pénale

200 Elles font même partie du droit fondamental à la protection des données tel qu'inscrit à l'article 8 de la Charte des droits fondamentaux de l'Union européenne.
201 Article 15 Convention 108+; article 51.1 RGPD.
202 Article 15.5 Convention 108+; article 52 RGPD.
203 Article 17 Convention 108+; Articles 60-61 RGPD.
204 Article 15.2.a et c Convention 108+ ; article 57.1.h RGPD.
205 Article 15.4 Convention 108+ ; article 57.1.f RGPD.
206 Article 15.4 Convention 108+ ; article 57.1.c RGPD.
207 Article 15.2.c Convention 108+.
208 Paragraphe 119 Rapport explicatif de la Convention 108+.
209 Article 83 RGPD.
210 Article 4 LPD.
211 Articles 49-50 LPD.
212 Article 51 LPD.

compétentes.[213] C'est aux tribunaux civils ou pénaux, voire administratifs que les personnes concernées doivent s'adresser. Les sanctions pénales ont d'ailleurs été renforcées dans la LPD par rapport au passé.[214] Les tribunaux pénaux pourront punir d'une amende pouvant aller jusqu'à 250.000 CHF la violation des différentes obligations instaurées par la LPD.[215] Ce plafond a été fixé bien plus bas que celui des amendes administratives du RGPD mais plus haut que pour les amendes pénales dans certains pays de l'UE (en Belgique l'amende pénale maximale équivaut à peu près à la moitié de l'amende suisse).

L. Conclusion

Le double dispositif européen de protection des données personnel, provenant du Conseil de l'Europe et de l'Union européenne, sert d'incontournable toile de fond pour le déploiement d'une législation de protection des données en Suisse.

La Convention 108 est le seul instrument juridiquement contraignant présentant le potentiel de devenir une norme universelle en matière de protection des données à caractère personnel. La révision de ce texte a conduit à l'adoption en 2018 du Protocole d'amendement 223, baptisé Convention 108+, qui a été signé par la Suisse mais n'a pas encore été ratifié par ce pays à ce jour.

Le processus de révision de la Convention a introduit dans le texte des éléments renforçant la protection des individus. Le premier de ces éléments est la formulation explicite du principe de proportionnalité à respecter à tous les stades du traitement des données et pour toutes les opérations effectuées avec les données. Ce principe était déjà présent dans la loi fédérale suisse de 1992, se rapportant principalement aux données faisant l'objet d'un traitement. Il a désormais une portée élargie et impacte aussi ce qui peut être fait avec les données.

D'autres améliorations majeures de la protection sont présentes dans les deux textes européens. Elles concernent les droits garantis à la personne concernée, notamment le droit de ne pas être soumis à une décision exclusivement automatisée (l'être humain ne doit pas être soumis à une machine), le droit de s'opposer au traitement des données personnelles et le droit de connaître le raisonnement qui sous-tend un traitement. L'autodétermination informationnelle signifie non seulement le droit de savoir, mais aussi le droit de comprendre ce qui est fait avec ses

213 Article 65 LPD ; cf. pour les traitements de données effectués par les organes fédéraux : « Le Conseil fédéral est arrivé à la conclusion qu'il n'est pas opportun de conférer au préposé la compétence de prononcer des sanctions administratives à l'encontre des organes fédéraux, au motif qu'une telle possibilité, qui existe dans d'autres pays, n'est pas conforme à notre tradition juridique. Le Conseil fédéral considère que la possibilité pour le préposé d'interdire ou de suspendre un traitement effectué par un organe fédéral, ainsi que le renforcement du volet pénal de la loi, constituent des mesures suffisantes. » (Message concernant la loi fédérale sur la révision totale de la loi fédérale sur la protection des données et sur la modification d'autres lois fédérales, FF 2017 6565, 6589).

214 Message concernant la loi fédérale sur la révision totale de la loi fédérale sur la protection des données et sur la modification d'autres lois fédérales, FF 2017 6565, 6597.

215 Article 61 LPD.

données. Les droits déjà existants ont été enrichis, comme le droit d'accès. Le RGPD a également introduit le nouveau droit à la portabilité des données. Toutes ces nouveautés ou ces enrichissements se retrouvent, avec les nuances évoquées dans les pages qui précèdent, dans la version de 2020 de la LPD.

De nouveaux devoirs apparus dans les deux textes européens ont été également intégrés dans la LPD, comme l'important devoir de transparence (présenté comme un droit à recevoir des informations dans le RGPD), celui de mettre en œuvre la *privacy by design* et *by default*, de prendre des mesures liées au principe d'*accountability*, de désigner un délégué ou conseiller à la protection des données, d'effectuer une analyse d'impact et celui de notifier les violations de données. Certaines de ces nouvelles obligations incombent aussi bien aux responsables du traitement qu'aux sous-traitants.

Le tableau résultant de la modernisation de la Convention 108 à Strasbourg et de l'adoption du RGPD à Bruxelles est clairement amélioré en ce qui concerne la protection des individus en Europe au vingt-et-unième siècle face au traitement de leurs données. La nature générale du texte de la Convention 108+ permet davantage de marge d'application que celle résultant du texte de l'UE. Mais contrairement au RGPD, la Convention 108+ couvre toutes les activités des secteurs privé et public. C'est là un atout essentiel de cet instrument juridique.

La réécriture de la LPD tenant compte des engagements qui découleront de la ratification par la Suisse du Protocole 223 a conduit à un renforcement de la protection des personnes physiques et de leur autodétermination informationnelle.