CERT

Jean-Philippe Dunand | Pascal Mahon (éds)

Vincent Carron | Valérie Défago Gaudin
Camille Dubois | Jean-Philippe Dunand
Anne-Sylvie Dupont | Sébastien Fanti
Christian Flueckiger | Karine Lempen
Marie Major | Estelle Mathis-Zwygart
Jean Christophe Schwaab | Camille Stauffer
Audrey Voutat | Jean-Philippe Walter
Catherine Weniger | Aurélien Witzig

La protection des données dans les relations de travail

CERT
Centre d'étude
des relations de travail

unine
UNIVERSITÉ DE NEUCHÂTEL
FACULTÉ DE DROIT

Schulthess
ÉDITIONS ROMANDES

La protection des données dans les relations de travail

Jean-Philippe Dunand | Pascal Mahon (éds)

Vincent Carron | Valérie Défago Gaudin
Camille Dubois | Jean-Philippe Dunand
Anne-Sylvie Dupont | Sébastien Fanti
Christian Flueckiger | Karine Lempen
Marie Major | Estelle Mathis-Zwygart
Jean Christophe Schwaab | Camille Stauffer
Audrey Voutat | Jean-Philippe Walter
Catherine Weniger | Aurélien Witzig

La protection des données dans les relations de travail

CERT
Centre d'étude
des relations de travail

Schulthess
ÉDITIONS ROMANDES
§ 2017

Citation suggérée de l'ouvrage : Jean-Philippe Dunand, Pascal Mahon (éds), *La protection des données dans les relations de travail,* Collection CERT, Genève/Zurich 2017, Schulthess Éditions Romandes

ISBN 978-3-7255-8646-2

www.schulthess.com

Diffusion en France : Lextenso Éditions, 70, rue du Gouverneur Général Éboué, 92131 Issy-les-Moulineaux Cedex

www.lextenso-editions.com

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

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

Table des matières

Table des abréviations ..... **XI**

Première partie – Principes généraux

Principes généraux de la protection des données et communications transfrontières dans le cadre des relations de travail **1**

Christian Flueckiger

Docteur en droit, Préposé cantonal (NE/JU) à la protection des données et à la transparence

Actions et procédure **25**

Aurélien Witzig

Docteur en droit, avocat, chargé d'enseignement à l'Université de Neuchâtel

Protection des données personnelles : contexte international et avant-projet de réforme du Conseil fédéral **47**

Camille Dubois

Avocate, juriste à l'Office fédéral de la justice

Accès aux documents officiels contenant des données personnelles et droit à la protection des données **77**

Jean-Philippe Walter

Docteur en droit, Préposé fédéral suppléant à la protection des données et à la transparence

Deuxième partie – Questions spécifiques

Protection des données des employés dans le cadre de transferts d'entreprises et de fusions **111**

Vincent Carron

Avocat, spécialiste FSA en droit du travail, LLM New York University

Catherine Weniger

Docteure en droit, avocate, spécialiste FSA en droit du travail

La confidentialité du salaire en droit privé du travail et dans la fonction publique **141**

Valérie Défago Gaudin

Avocate, docteure en droit, professeure à l'Université de Neuchâtel

Jean-Philippe Dunand

Avocat, docteur en droit, professeur à l'Université de Neuchâtel

Audrey Voutat

MLaw, avocate, assistante-doctorante à la Faculté de droit de Neuchâtel

La protection des données confiées aux assureurs **195**

Anne-Sylvie Dupont

Docteure en droit, avocate, professeure aux Universités de Neuchâtel et de Genève

Protection des données informatiques **229**

Sébastien Fanti

Avocat, Préposé cantonal valaisan à la protection des données et à la transparence

Protection des données et discrimination lors de la procédure de recrutement **269**

Karine Lempen

Docteure en droit, professeure à l'Université de Genève

Le droit d'accès de l'employé à son dossier personnel **287**

Marie Major

Avocate, greffière-juriste auprès du Tribunal des prud'hommes du canton de Genève

La surveillance des travailleurs sous l'angle des articles 328b CO et 26 OLT 3 ..... **309**

Estelle Mathis-Zwygart

Docteure en droit, avocate, greffière-rédactrice au Tribunal régional du Littoral et Val-de-Travers

La licéité de l'évaluation et du « forced ranking » en droit suisse du travail **325**

Jean Christophe Schwaab

Juriste, Conseiller national

La communication de données à un organe paritaire dans le cadre d'un contrôle CCT **343**

Camille Stauffer

Secrétaire juridique auprès de la Commission paritaire genevoise du Gros œuvre

SÉBASTIEN FANTI

Protection des données informatiques

« Prétendre que votre droit à une sphère privée
n'est pas important parce que vous n'avez rien à cacher
n'est rien d'autre que de dire
que la liberté d'expression n'est pas essentielle,
car vous n'avez rien à dire. »
— Edward Snowden

Sommaire Page

I. Introduction 230

II. Le cadre normatif applicable en droit du travail 231
- A. Liminairement et contextuellement 231
- B. Le Règlement européen sur la protection des données personnelles 232
- C. Panorama non exhaustif des normes fédérales applicables 235
- D. Le guide relatif aux mesures techniques et organisationnelles de la protection des données publié par le Préposé fédéral 246
- E. Le guide pour le traitement des données personnelles dans le secteur du travail (traitement par des personnes privées), émis par le Préposé fédéral 248
- F. Le droit cantonal : l'exemple de la loi valaisanne sur l'information du public, la protection des données et l'archivage 249
- G. Casuistique 250
- H. Windows 10 254
- I. Quelques exemples d'utilisation des moyens techniques en vue d'une amélioration de la protection des données 256

III. Les méthodes alternatives 258
- A. Les normes ISO 258
- B. Les norme ISO applicables en matière de protection des données 259

IV. La protection des données informatiques par l'intelligence artificielle (IA) et ses garde-fous 260
- A. L'état de la technologie et les développements en matière de cybersécurité 260
- B. Le drapeau rouge d'Alan Turing 261

V. Conclusions et perspectives 262

Annexe 264

Bibliographie 266

I. Introduction

La protection des données informatiques dans le cadre des relations de travail constitue une tâche titanesque. Par nature, l'activité d'une entreprise, quelle que soit sa taille évolue, ce qui génère une impérieuse nécessité de révision régulière de la politique de protection des données informatiques, rarement diligentée toutefois. Même dans une petite PME (où la tâche semble plus aisée), la gestion des données s'apparente au tonneau des Danaïdes : administration déficiente des droits d'accès, partage natif des données entre les collaborateurs, absence de procédure de contrôle des flux de données, etc. Ce n'est que lorsqu'un conflit survient, que les manquements apparaissent, au grand jour, avec des conséquences importantes et variables, en fonction notamment des capacités probatoires de chacun. Le risque pour chacune des parties à la relation de travail se matérialise alors avec des conséquences économiques, voire parfois disciplinaires ou pénales. La présente contribution a pour objectif d'appréhender différentes hypothèses à l'aune des dispositions légales en vigueur et envisagées et d'anticiper les processus de travail en réfléchissant aux garde-fous nécessaires. Car les processus sont en mutation profonde.

Stephen Hawking[1] soutenait dans une tribune publiée par le Guardian, le 1er décembre 2016[2], que l'automatisation et l'intelligence artificielle vont décimer les emplois de la classe moyenne, aggravant ainsi les inégalités sociétales et engendrant un risque d'importants bouleversements politiques[3].

Trois des dix plus grands employeurs du monde remplacement depuis près d'un an leurs collaborateurs par des robots[4].

Les données ne vont pas échapper, quant à leur traitement et à leur protection, à ce que les économistes qualifient de quatrième révolution industrielle[5]. La tentation est en effet grande de les confier à des « *processus intelligents et objectivables* » et de s'extraire ainsi des conflits humains. Si tel devait être le cas, il conviendrait alors de prévoir un régime

---

1 Stephen Hawking est un physicien théoricien et cosmologiste britannique aux talents protéiformes : http://www.hawking.org.uk/about-stephen.html.

2 https://www.theguardian.com/commentisfree/2016/dec/01/stephen-hawking-dangerous-time-planet-inequality.

3 Cf. notamment https://www.letemps.ch/economie/2016/10/16/on-pourrait-imaginer-quun-robot-refuse-payer-impots.

4 http://www.businessinsider.fr/uk/clsa-wef-and-citi-on-the-future-of-robots-and-ai-in-the-workforce-2016-6/.

5 Cette quatrième révolution industrielle est caractérisée par des développements sans précédent dans la génétique, l'intelligence artificielle, la robotique, la nanotechnologie, l'impression 3D, et la biotechnologie, cf. http://www.businessinsider.fr/uk/wef-davos-report-on-robots-replacing-human-jobs-2016-1/.

juridique adéquat et pertinent, permettant notamment de discerner l'intervention automatisée et de la signaler comme telle[6]. C'est donc un régime de protection évolutif et protéiforme qui doit faire l'objet du présent examen.

II. Le cadre normatif applicable en droit du travail

A. Liminairement et contextuellement

Ainsi que le relève pertinemment BERTIL COTTIER[7], il existe une difficulté d'établissement de standards universels de protection de la vie privée et/ou des données personnelles[8]. Cette situation a généré des développements différenciés entre l'Europe et le reste du monde, permettant ainsi à des modèles alternatifs de s'immiscer[9]. Singulièrement, près de 50 ans après l'apparition des premières législations topiques en matière de protection des données, celles-ci n'ont guère prospéré que sur le continent européen[10].

Hors d'Europe, à l'exception du Canada[11], de l'Australie[12] et de la Nouvelle-Zélande[13], les législations topiques et dignes de ce nom sont rarissimes dans les pays dits développés. Les États-Unis, par exemple, s'opposent fermement à une approche généraliste identique à celle prévalant en Europe, car cela entraverait la bonne marche des affaires[14]. Les motifs pour lesquels la privacité n'a pas gagné ses lettres de noblesse outre-Atlantique sont certes plurifactoriels[15], mais l'argument économique demeure fondamental. Quant à l'Asie, elle a connu des développements intéressants depuis quelques années (notamment au Japon, à Singapour, à Hong-kong et en Corée du Sud), sans toutefois assortir les normes des moyens adéquats de mise en œuvre des standards de protection[16].

---

6 En application du principe de prévention, ainsi que nous le verrons ci-après, cf. § 4.2.

7 COTTIER, p. 268.

8 Ce constat est également valable plus généralement pour l'ensemble du droit de l'Internet et des nouvelles technologies, cf. à cet égard, ANCELLE, pp. 195 ss.

9 Cf. § 3.1 et § 3.2.

10 A l'exception de la Biélorussie, tous les pays du continent ont adopté des législations en matière de protection des données. Il faut toutefois reconnaître que leur spectre de protection diverge.

11 Pour un panorama des normes en matière de protection des données : http://www.bdp.parl.gc.ca/content/lop/researchpublications/prb0744-f.htm.

12 Pour une présentation des normes : https://www.oaic.gov.au/privacy-law/.

13 Voici le lien vers les normes applicables dans ce pays : https://www.privacy.org.nz/the-privacy-act-and-codes/privacy-act-and-codes-introduction/.

14 Pour une approche comparative, ALO.

15 Pour un exposé détaillé de ces motifs, cf. COTTIER, pp. 259 à 261.

16 Cf. COTTIER, N 2, pp. 260 à 261 et les références citées.

Ce bref exposé préliminaire a pour but de mettre en exergue l'existence de normes fondamentalement différentes[17] et, partant, de risques qui doivent être appréhendés avec finesse, judicieusement. La communication instantanée, l'interconnexion globale et permanente nécessitent assurément de tenir compte dans l'analyse et la méthodologie de protection des données informatiques de tous les corpus juridiques. En clair, il pourrait ne pas[18] suffire de respecter le droit suisse lequel prévoit déjà un certain nombre de garde-fous lors de la transmission de données à l'étranger. Ainsi que le mettent en exergue JULIETTE ANCELLE ET MICHEL JACQUARD[19], l'identification des possibles transferts de données internationaux est essentielle, car ceux-ci sont susceptibles de déclencher l'application de règles et d'obligations spécifiques : à titre exemplatif, la transmission de données à des tiers ne peut intervenir à n'importe quelle condition[20] et la transmission de données à l'étranger s'avérerait illicite si elle risquait de menacer gravement la personnalité des personnes concernées[21]. Dès l'instant où des données se disséminent[22] hors des frontières helvétiques, le risque devient exponentiel. Il suffit à cet égard que les données, bien que stockées en Suisse, soient accessibles depuis un pays tiers.

Encore faudra-t-il donc s'assurer, dans le cadre de l'activité économique déployée, que les données ne sont pas également soumises à des normes étrangères et dans l'affirmative que celles-ci sont respectées. À défaut, les mauvaises surprises pourraient sanctionner une approche juridique et prudentielle déficiente, soit locale.

B. Le Règlement européen sur la protection des données personnelles

Dans le contexte international éclaté dont il a été question, le Règlement européen sur la protection des données personnelles[23] mérite une attention particulière, en raison

---

17 Pour un aperçu synthétique de l'état de la protection des données dans le monde, cf. https://www.edoeb.admin.ch/datenschutz/00626/00753/index.html?lang=fr&download=NHzLpZeg7t,lnp6I0NTU042l2Z6ln1ae2IZn4Z2qZpnO2Yuq2Z6gpJCDdXt3fmym162epYbg2c_JjKbNoKSn6A-- ; cf. également COTTIER, Quoi de Neuf à l'Etranger, pp. 67 à 85.

18 Plus!

19 ANCELLE/JACCARD, p. 371.

20 Cf. art. 10a de la loi fédérale sur la protection des données du 19 juin 1992 (LPD, RS 235.1) et WINKLER, p. 111.

21 Cf. art. 6 al. 1 LPD.

22 Au sens large du terme.

23 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

notamment de l'intensité de nos échanges avec nos voisins européens, de l'amplitude des modifications qu'il comporte et de l'amplification des sanctions à prononcer en cas de violation des normes en matière de protection des données. À cela s'ajoute le caractère eurocompatible de la législation helvétique, ainsi que les effets extraterritoriaux de la réglementation[24].

Ce nouveau règlement, paru au Journal officiel de l'Union européenne le 4 mai 2016, entrera en vigueur le 25 mai 2018. Parmi ses nombreuses nouveautés[25], il convient de mettre en exergue l'introduction d'un régime de sanctions très dissuasif : les sanctions en cas de non-conformité deviennent extrêmement lourdes, puisqu'elles peuvent s'élever à 20'000'000 d'euros ou 4% du chiffre d'affaires du groupe auquel le contrevenant appartient, selon le montant le plus élevé.

Sous l'égide de l'ancienne directive 95/46, les entreprises suisses étaient relativement à l'abri des dispositions européennes en matière de protection des données. Principalement inquiétées en cas de traitement de données effectué dans le cadre des activités d'un établissement sur le territoire d'un État membre ou, à défaut d'établissement, de recours à des moyens de traitement situés sur le territoire d'un État membre. Néanmoins, l'entreprise suisse concernée ne se voyait pas appliquer une législation européenne unifiée, mais bien le droit des États membres desquels elle remplissait ses conditions.

Aujourd'hui, la donne est tout autre. L'unification du droit européen par le nouveau RGPD ne s'est pas contentée de renforcer la position des personnes concernées par un traitement de données, mais il a considérablement étendu son champ d'application territorial. Les entreprises suisses concernées sont nombreuses et vont devoir s'adapter rapidement aux nouvelles exigences du règlement, tant il est vrai qu'une période transitoire de moins de 2 ans est, en fonction de la taille de l'entreprise, infinitésimale. Certaines dispositions du RGPD nécessiteront en effet probablement d'importants changements dans l'organisation des entreprises.

Quelles sont les entreprises suisses concernées ? L'**établissement** au sein de l'Union reste un critère justifiant l'application du RGPD. Il suffit qu'au cours de l'activité de celui-ci un

---

données), abrégé ci-après RGPD. Le RGPD est accessible à cette adresse : http://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX%3A32016R0679.

24 ANCELLE/JACCARD, p. 369.

25 Voici quelques-unes des nouveautés figurant dans ce texte (une présentation des principales modifications du RGPD figure en annexe au présent texte) : protection des données par conception et par défaut, nécessité dans certaines circonstances de conduire une analyse d'impact relative à la Protection des Données (AIPD), désignation obligatoire d'un Délégué à la Protection des Données (DPD) dans certaines situations, obligation de déclarer une violation des données à très brève échéance, etc. ; pour de plus amples informations sur les nouveautés introduites par le RGPD, cf. https://www.cnil.fr/fr/reglement-europeen-sur-la-protection-des-donnees-ce-qui-change-pour-les-professionnels.

traitement de données soit effectué (peu importe qu'il ait lieu ou non dans l'Union). Si cela peut concerner les entreprises suisses qui font partie d'un groupe de sociétés dont une partie est établie dans l'UE, le RGPD se distingue de l'ex-directive en ajoutant que l'établissement d'un sous-traitant au sein de l'Union est également concerné. Cela signifie qu'en cas de localisation du **sous-traitant** dans l'UE, l'application du RGPD sera justifiée pour les modalités de la délégation, mais également pour l'intégralité du traitement.

En dehors de l'établissement, il suffit qu'une entreprise cible également la clientèle européenne. C'est-à-dire que dans le cadre d'une **offre de biens ou de services** (gratuit ou non), il traite des données de clients (à condition qu'ils soient des personnes physiques) se trouvant sur le territoire de l'UE. On considérera l'existence d'une telle offre par un ensemble d'indices qui montre que cette dernière n'est pas limitée à la Suisse (langue utilisée, devise proposée, mention de clients ou d'utilisateurs dans l'UE, etc.).

Est aussi concernée l'entreprise qui **suit le comportement** de personnes présentes sur le territoire de l'UE, à condition que ce comportement ait lieu au sein de l'UE. Cette catégorie englobe évidemment toutes les techniques de profilage ou de suivi de l'activité des utilisateurs et clients. Il n'est à cet égard plus nécessaire de démontrer l'usage d'un « moyen de traitement », tel que les cookies et JavaScript, qui justifiait l'application de l'ancienne directive. À présent, est concerné également le profilage de l'utilisateur réalisé à partir de l'observation des activités online de ce dernier (comme par exemple sur les réseaux sociaux).

Pour ces deux derniers cas d'assujettissement au règlement, il est très important de relever que comme l'établissement, cela concernera tant les traitements de données de l'entreprise suisse que celui du **sous-traitant**. Cela signifie que le RGPD mentionne explicitement que les entreprises suisses ne pourront pas s'exonérer par la sous-traitance de tout ou partie du traitement.

Enfin, le RGPD réserve encore son application au cas où l'entreprise serait établie en un lieu où le droit d'un État membre est applicable en vertu des règles sur le droit international public[26].

[26] Pour de plus amples informations relativement à l'application de l'art. 3 du RGPD, cf. COTON/HENROTTE, pp. 171-217 et 73-104.

En bref donc, le champ d'application territorial du RGPD[27] s'avère complexe à circonscrire et par nature évolutif[28]. Le principe de précaution devra donc prévaloir pour toutes les sociétés et dans le doute, celles-ci devront s'astreindre à une évaluation de la maturité de leur organisation en matière de protection des données.

C. Panorama non exhaustif des normes fédérales applicables

En droit du travail, c'est l'article 328b du Code des obligations[29] qui est déterminant pour le traitement des données relatives aux collaborateurs. Son libellé est le suivant : « *L'employeur ne peut traiter des données concernant le travailleur que dans la mesure où ces données portent sur les aptitudes du travailleur à remplir son emploi ou sont nécessaires à l'exécution du contrat de travail. En outre, les dispositions de la loi fédérale du 19 juin 1992 sur la protection des données sont applicables* »[30]. Les rapports de travail génèrent une collecte et un traitement des nombreuses données personnelles du travailleur, collecte de longue durée. À cela s'ajoute le fait que le travailleur dépend, en fait et en droit, en raison du devoir de subordination caractéristique de son statut de son employeur[31].

---

27 L'art. 3 RGPD (Champ d'application territorial) a la teneur suivante :

1. *Le présent règlement s'applique au traitement des données à caractère personnel effectué dans le cadre des activités d'un établissement d'un responsable du traitement ou d'un sous-traitant sur le territoire de l'Union, que le traitement ait lieu ou non dans l'Union.*
2. *Le présent règlement s'applique au traitement des données à caractère personnel relatives à des personnes concernées qui se trouvent sur le territoire de l'Union par un responsable du traitement ou un sous-traitant qui n'est pas établi dans l'Union, lorsque les activités de traitement sont liées :*

   a) à l'offre de biens ou de services à ces personnes concernées dans l'Union, qu'un paiement soit exigé ou non desdites personnes ; ou

   b) au suivi du comportement de ces personnes, dans la mesure où il s'agit d'un comportement qui a lieu au sein de l'Union.
3. *Le présent règlement s'applique au traitement de données à caractère personnel par un responsable du traitement qui n'est pas établi dans l'Union mais dans un lieu où le droit d'un État membre s'applique en vertu du droit international public.*

28 En fonction de la jurisprudence qui sera rendue.

29 RS 220 ; l'art. 328 CO qui énonce le régime général de la protection de la personnalité du travail est complété par l'article 328b CO qui contient les règles spécifiques relatives au traitement des données personnelles du travailleur.

30 Pour une analyse détaillée de cette disposition légale : cf. notamment MEIER, N 2020, p. 646.

31 Sur la *ratio legis*, cf. Message concernant la loi fédérale sur la protection des données (LPD) du 23 mars 1998, FF 1988 421 (494).

Les données traitées dans le cadre de l'activité professionnelle peuvent constituer des données sensibles[32] ou des profils de personnalité[33]. L'employeur, en sa qualité de maître de fichier, doit protéger ces données contre tout traitement non autorisé en vertu de l'article 7 LPD. Et sa tâche se complexifie avec la multiplication des outils informatiques. Le Bring Your Own Device (BYOD), soit l'utilisation d'équipements personnels dans un contexte professionnel en est une excellente illustration, dès lors qu'il oblige l'employeur à assurer la sécurité d'appareils qui ne lui appartiennent pas, ce qui relève quasiment de l'impossible[34] ! Le risque d'atteintes importantes à la personnalité des travailleurs est aujourd'hui amplifié[35].

Comme le relève le Professeur JEAN-PHILIPPE DUNAND[36], l'employeur a tout intérêt à recourir à diverses mesures techniques et organisationnelles qui limiteront les abus ou les risques de l'entreprise[37].

Parmi les principes fondamentaux régissant le traitement des données personnelles, figure celui de la sécurité des données. Il ne suffit en effet pas d'édicter des règles juridiques pour assurer une pleine protection des données à caractère personnel. Il faut encore que des précautions matérielles soient effectivement prises par le responsable du traitement pour prévenir les accès ou les utilisations illégitimes des données, autant par accident que par malveillance[38].

S'agissant des mesures techniques et organisationnelles de la protection des données, le siège de la matière figure dans la loi fédérale sur la protection des données du 19 juin 1992[39] (abrégée ci-après LPD), ainsi que dans l'Ordonnance relative à la loi fédérale sur la protection des données du 14 juin 1993[40] (abrégée ci-après OLPD). La LPD et son ordonnance d'application n'impliquent pas simplement de se conformer à certaines restrictions, mais nécessitent l'adoption de mesures concrètes (« organisationnelles et techniques »)[41] et appropriées. Il s'agit donc de se montrer actif, voire proactif pour anticiper les difficultés qui pourraient survenir.

---

32 Cf. art. 3 let. c LPD.

33 Cf. art. 3 let. d LPD.

34 A cet égard, cf. FANTI, pp. 165 à 203.

35 Pour des exemples de matérialisation du risque : DUNAND, pp. 56 ss.

36 DUNAND, p. 69.

37 Même s'il faut convenir que les sanctions de la violation de l'art. 328*b* CO sont rares.

38 Conseil de l'Europe, La protection des données à caractère personnel collectées et traitées à des fins statistiques, Recommandation n° R (97) 18 adoptée par le Comité des Ministres du Conseil de l'Europe le 30 septembre 1997 et exposé des motifs, p. 94.

39 RS 235.1.

40 RS 235.11.

41 ANCELLE/JACCARD, pp. 370 ss.

L'article 7 LPD intitulé « *Sécurité des données* »[42] prescrit à son alinéa premier que les données personnelles[43] doivent être protégées contre tout traitement non autorisé par des mesures organisationnelles[44] et techniques appropriées. Le Conseil fédéral édicte des dispositions plus détaillées sur les exigences minimales en matière de sécurité des données (art. 7 al. 2 LPD). La sécurité des données est la pierre angulaire de l'édifice de protection des données, dès lors qu'elle permet d'assurer la confidentialité, la disponibilité et l'intégrité des données. On ne saurait toutefois exiger une sécurité absolue, car il est tout simplement impossible de se prémunir contre toutes les éventualités.

Les articles 8 à 12 et 20 à 22 OLPD concrétisent pour le **secteur privé**[45] et le **secteur public**[46] ces exigences minimales évoquées à l'article 7 LPD[47].

Le responsable de traitement doit assurer la sécurité des données en prenant les mesures techniques et organisationnelles appropriées pour éviter tout traitement non autorisé et notamment établir un règlement de traitement pour les traitements présentant un risque particulier d'atteintes aux droits et libertés fondamentales, de journaliser les traitements de données sensibles ou d'informer les destinataires de l'actualité et de la fiabilité des données personnelles transmises[48].

Les articles 8 à 12 OLPD définissent **pour le secteur privé** un cadre minimum à atteindre en matière de sécurité des données, cadre proportionné par la mise en balance des différents intérêts en présence (art. 8 al. 2 OLPD). Une différenciation s'opère en effet en fonction des finalités du traitement, de la nature des données traitées, de l'étendue du traitement et des risques encourus par les personnes concernées. Dans ce contexte, il doit

---

42 Pour un cas récent permettant d'illustrer la problématique de la sécurité des données, cf. CHABOT.

43 Selon l'art. 3 let. a LPD, on entend par données personnelles, toutes les informations qui se rapportent à une personne identifiée ou identifiable.

44 Une mesure technique est directement liée au système d'information lui-même et le concerne directement. Une mesure organisationnelle se rapporte plus à l'entourage du système, en particulier aux personnes qui l'utilisent. La combinaison des deux permet seule d'éviter la destruction et la perte des données, ainsi que les erreurs, la falsification, les accès non autorités, etc.

45 Art. 8 à 12 OLPD.

46 Art. 20 à 22 OLPD.

47 BAERISWYL, N 34-35 *ad* art. 7 LPD, p. 95.

48 WALTER, p. 118.

être tenu compte de l'état de la technique[49] et dans une moindre mesure des coûts et de la capacité financière de l'entreprise concernée[50].

Sous réserve de l'article 10 OLPD qui introduit une obligation de journaliser certains traitements portant sur des données sensibles ou des profils de personnalité, l'ordonnance ne prescrit aucune mesure technique particulière, telle que mot de passe, autres mesures techniques d'identification, chiffrement des données, etc. Il appartient donc au maître du fichier d'analyser le risque et de l'appréhender à l'aune des éléments précités. La lecture du message relatif à la LPD permet de constater que le législateur entendait, à l'aune de la grande diversité des techniques de traitement des données, renoncer à réglementer dans le détail les mesures de sécurité envisageable[51]. Soin était donc laissé à ceux qui traitent les données, respectivement aux organisations professionnelles qui les représentent de déterminer les mesures de sécurité propres à leur domaine d'activité et de prendre les dispositions adéquates. Le choix opéré avait notamment pour but de contraindre à une réévaluation périodique (art. 8 al. 3 OLPD), compte tenu du caractère évolutif du processus et du développement de la technique. Selon la jurisprudence[52], un *update* des mesures de sécurité devrait intervenir tous les ans, sauf circonstances extraordinaires, c'est-à-dire par exemple une adaptation des normes légales ou l'apparition d'une nouvelle menace[53]. Il va sans dire que dans le contexte actuel, avec une révision en cours de la LPD et l'introduction d'un nouveau cadre au niveau européen, qu'une évaluation de l'état de maturité en matière de protection des données devra être diligentée avec soin.

Force est toutefois de constater que depuis l'adoption de la loi, l'autorégulation n'a guère prospéré et que les doutes continuent d'assaillir les personnes astreintes à traiter des données personnelles[54], entravant *de facto* un développement aisé et harmonieux de bonnes pratiques.

L'article 8 alinéa 1 OLPD énumère les risques contre lesquels il y a lieu de protéger les données, dans la mesure où cela est nécessaire et propre à garantir la protection des

---

49 Cf. art. 8 al. 2 let. d OLPD, étant précisé que les mesures techniques et organisationnelles doivent fait l'objet d'un réexamen périodique notamment à l'aune du développement technique.

50 Ce dernier élément ne devant toutefois intervenir qu'à titre accessoire. A défaut, il suffirait à une entreprise d'exciper d'un manque de ressources pour ne pas avoir à respecter les normes en matière de protection des données ; cf. à cet égard FANTI, p. 180.

51 Message concernant la loi fédérale sur la protection des données (LPD) du 23 mars 1998, FF 1988 II 421 (459 et 460).

52 ATAF A-4467/2011 du 10 avril 2002, c. 9.

53 A l'instar d'un nouveau virus.

54 WALTER, p. 119 ; cf. également ANCELLE/JACCARD, p. 369.

données, c'est à dire la protection de la personnalité des personnes. Il s'agit en particulier[55] des risques suivants :

- destruction accidentelle ou non autorisée ;
- perte accidentelle ;
- erreurs techniques ;
- falsification, vol ou utilisation illicite ;
- modification, copie, accès ou autres traitements non autorisés.

La finalité des mesures techniques et organisationnelles, notamment en présence de fichiers automatisés ou de systèmes d'informations automatisés, est d'éviter que ces fichiers ou ces systèmes ne permettent plus que ce qu'ils ne doivent[56]. À cet effet, l'article 9 al. 1 OLPD énonce une série d'objectifs à atteindre, en particulier lors de traitements automatisés. À dessein, ces mesures ne se limitent pas à l'existence d'un fichier, puisque la tendance actuelle va vers une plus grande dispersion des informations dans de vastes systèmes d'informations répondant à des schémas d'organisation différents, mais qui permettent néanmoins un usage par personne concernée. Par rapport à ces nouvelles tendances informatiques et télématiques, la notion de fichier est dépassée.

Les objectifs énoncés à l'article 9 alinéa 1 OLPD sont au nombre de huit[57]. Ces objectifs doivent servir de *fil* rouge aux entreprises. Ils doivent être réalisés conformément au

---

55 L'énumération est exemplative et non exhaustive.

56 Commentaire de l'Office fédéral de la justice (OFJ) à l'appui de l'ordonnance du 14 juin 1993 relative à la loi fédérale sur la protection des données, p. 9, disponible en ligne sur : https://www.edoeb.admin.ch/org/00129/index.html?lang=fr&download.

57 1. Contrôle à l'entrée des installations : il s'agit ici de prendre des mesures propres à éviter que des personnes non autorisées aient accès aux installations utilisées pour le traitement de données personnelles, notamment l'accès aux locaux où sont situés les ordinateurs. Cet objectif ne vise pas uniquement l'accès à un ordinateur central, mais également les périphériques, tels que les terminaux.
2. Contrôle des supports de données : ce contrôle doit permettre d'éviter qu'une personne non autorisée puisse lire, copier, modifier ou éloigner des supports de données. En particulier, il faut veiller à empêcher que des données puissent être déchargées de manière incontrôlée sur des supports de données. Un support de données est un support physique sur lequel des données peuvent être transcrites (papier, image, carte perforée, support magnétique, disque dur, disquette, bande, disque compact, carte/support optique, etc.). N'est considéré comme support de données que le support indépendant c.à.d. qui n'est pas intégré au fichier, à l'ordinateur, au système informatique ou à l'installation principale de conservation des données.
3. Contrôle de transport : cet objectif tend à éviter qu'une personne non autorisée puisse prendre connaissance des données (copier, modifier, effacer) lors de leur communication. Le destinataire des informations doit également avoir l'assurance que les données qu'il reçoit sont bien celles qui lui ont été envoyées et qu'aucun tiers ne les a interceptées de manière illicite. Ainsi, en cas de risque particulièrement élevé d'atteinte à la vie privée et aux droits des personnes concernées, notamment du

principe de proportionnalité et tenir compte, comme pour l'ensemble des autres mesures de sécurité, des finalités, de la nature et de l'étendue du traitement, de l'évaluation des risques potentiels pour les personnes concernées et du développement actuel[58]. Un système d'informations en matière de protection de l'État ou un fichier de santé ne *répondra* pas aux mêmes niveaux de sécurité qu'un fichier d'adresses.

L'article 9 alinéa 2 énonce une règle relative à l'organisation des fichiers. Ceux-ci doivent être organisés de manière à permettre aux personnes concernées d'exercer leur droit d'accès. Cela implique en particulier que des mesures techniques et organisationnelles soient prises pour leur délivrer le contenu des données les concernant.

La journalisation des traitements automatisés de données sensibles ou de profils de la personnalité (art. 10 OLPD) a pour but d'opérer des vérifications *a posteriori.* Elle n'interviendra que dans la mesure où le maître de fichier n'a pas pris d'autres mesures

---

fait que des données sensibles ou des profils de la personnalité sont communiqués, on recourra à des méthodes de chiffrement des données ou à des mesures offrant une sécurité équivalente.

4. Contrôle de communication : cette mesure doit permettre d'identifier les destinataires des données, c'est-à-dire vérifier et constater à quelles personnes ou organes des données sont communiquées. Elle doit permettre de contrôler au besoin au moyen de quelle installation et à qui les données ont été communiquées, notamment en journalisant les communications. La journalisation ne doit pas toujours être introduite, mais il faut être en mesure d'examiner le déroulement des opérations.

5. Contrôle de mémoire : cet objectif tend à empêcher qu'une personne non autorisée puisse avoir accès à un fichier ou à un système de traitement automatisé, et en particulier prendre connaissance du contenu de la mémoire (unité fonctionnelle qui peut recevoir, conserver et restituer des données), le modifier ou l'effacer. Il faut ainsi introduire des mesures afin que seules les personnes autorisées puissent utiliser les données enregistrées dans le fichier ou le système de traitement automatisé et ce dans les limites de leur autorisation.

6. Contrôle d'utilisation : par cet objectif, on veut éviter qu'une personne non autorisée ne puisse utiliser un système de traitement automatisé, notamment en recourant à des installations de communication des données. Il s'agit en particulier d'empêcher des tiers de pénétrer dans le système.

7. Contrôle d'accès : par cet objectif, il faut garantir que seules les personnes autorisées ont accès aux seules données dont elles ont besoin pour l'accomplissement de leurs tâches. Ainsi, le maître du fichier doit délivrer des autorisations d'accès différenciées en fonction des tâches que chaque utilisateur est appelé à exécuter. Ces autorisations d'accès donnent le droit de traiter des données dans une mesure préalablement déterminée et pour une finalité prédéfinie. Elles doivent en particulier décrire la nature et l'étendue des accès.

8. Contrôle de l'introduction : cet objectif tend à assurer qu'un contrôle a posteriori des données introduites dans le fichier ou le système soit possible. Ce contrôle doit porter également sur la personne qui procède à l'introduction des données et sur le moment où l'opération a été effectuée. Il s'agit ici de permettre un suivi de l'introduction des données. Ce suivi ne nécessite pas obligatoirement une journalisation. L'introduction doit cependant pouvoir être contrôlée à l'aide des documents à disposition.

[58] A titre exemplatif, un système d'informations en matière de protection de l'Etat ou un fichier de santé ne répondra pas aux mêmes niveaux de sécurité qu'un fichier d'adresses.

préventives[59]. Le PFPDT est en droit de recommander la journalisation pour d'autres traitements lorsqu'ils présentent un risque élevé d'atteinte à la vie privée et aux droits des personnes concernées (art. 10 al. 1 *in fine* OLPD)[60]. La vérification va porter sur le respect des finalités du traitement de données pour lesquelles celles-ci ont été collectées ou communiquées[61]. Il n'est toutefois pas nécessaire de tout journaliser, le principe de proportionnalité devant évidemment trouver application[62]. Les procès-verbaux de journalisation servent à contrôler que les dispositions de protection des données ont été respectées. Ils ne doivent dès lors être rendus accessibles qu'aux seuls organes ou personnes chargés de vérifier l'application de ces dispositions, notamment le préposé fédéral et les organes internes de contrôle (responsables de la protection et de la sécurité des données dans l'entreprise ou dans une unité administrative). Ces procès-verbaux doivent être conservés durant une année sous une forme permettant d'effectuer le contrôle, c'est-à-dire qu'ils ne doivent en particulier pas pouvoir être modifiés[63].

L'article 11 OLPD prévoit quant à lui l'obligation d'élaborer un règlement de traitement[64] pour les fichiers automatisés du secteur privé soumis à déclaration conformément à l'article 11a alinéa 3 LPD. Le maître du fichier qui traite des données sensibles ou des profils de la personnalité ou qui communique régulièrement des données personnelles à des tiers est en principe tenu de déclarer ses fichiers et d'élaborer un règlement. Il sera toutefois délié de son obligation d'élaborer un règlement si son fichier tombe sous le coup d'une des exceptions prévues à l'article 11a alinéa 5 lettre b à d, LPD. En revanche s'il désigne un conseiller à la protection des données (art. 11a al. 5 let. e LPD) ou s'il souhaite obtenir un label de qualité en matière de protection des données, il devra élaborer un

---

59 A titre d'exemples de mesures préventives, on peut citer la séparation fonctionnelle entre les données personnelles et les programmes, les accès différenciés en fonction des utilisateurs et des tâches à accomplir, les codes d'accès, le principe des 4 yeux, etc.

60 Ce peut être le cas de fichiers ou de traitements qui sans contenir des données sensibles au sens de l'art. 3 let. c LPD présentent un certain degré de sensibilité notamment du fait du domaine dans lequel ils sont gérés (assurances, agence de renseignements, etc.) et de la configuration du système d'informations, en particulier lors de l'accès aux données par procédure d'appel.

61 Il convient en particulier de vérifier que les données ne sont pas utilisées à des fins non prévues ou non compatibles.

62 Cf. art. 4 al. 2 LPD et 8 al. 2 OLPD.

63 Commentaire de l'Office fédéral de la justice (OFJ) à l'appui de l'ordonnance du 14 juin 1993 relative à la loi fédérale sur la protection des données, p. 11, étant précisé que ce commentaire peut être consulté à cette adresse : https://www.edoeb.admin.ch/org/00129/index.html?lang=fr&download.

64 Pour un exemple de règlement relatif au traitement des données, cf. https://www.concordia.ch/fr/concordia/ueber_uns/datenschutz/_jcr_content/slot2par/download/file.res/06_Bearbeitungsreglement%20Version%201.2_06.08.15_f_PDF.pdf.

règlement même s'il est délié de son obligation de déclaration. Il en va de même lorsque des données sont traitées en vertu d'une obligation légale (art. 11a al. 5 let. a LPD).

Le règlement de traitement doit être conçu comme une documentation ou un manuel géré par le maître de fichier[65]. Ce règlement donne des informations sur l'organisation interne du maître du fichier, sur l'organisation et la structure dans laquelle se situe le fichier ou le système de traitement automatisé. Il décrit en particulier les procédures de traitement et de contrôle des données. Il comprend des documents relatifs à l'élaboration, à la planification et à la gestion du fichier et des moyens informatiques mis en œuvre. Ce règlement doit être régulièrement mis à jour et tenu[66] à disposition du préposé ou du conseiller à la protection des données au sens de l'article 11a alinéa 5 lettre e LPD sous une forme qui leur soit intelligible.

L'article 12 OLPD prévoit qu'avant la communication des données, le destinataire des données soit renseigné sur l'actualité et la fiabilité des données. Ainsi, dans la mesure où cela ne ressort pas des circonstances ou des données elles-mêmes, la personne privée qui communique indiquera en particulier la date de la dernière mise à jour et précisera si les données sont sûres ou incertaines quant à leur exactitude[67]. Elle est également dans l'intérêt de la personne qui communique, laquelle engage sa responsabilité si elle communique des données fausses.

S'agissant du **secteur public**, les mesures techniques et organisationnelles figurent aux articles 20 à 22 OLPD.

L'article 20 prévoit que les organes fédéraux responsables du traitement et du fichier[68] prennent des mesures techniques et organisationnelles propres à protéger la personnalité et les droits fondamentaux des personnes qui font l'objet d'un traitement de données[69]. Ces mesures sont identiques à celles prescrites pour le secteur privé[70].

Non seulement pour des raisons financières et d'efficacité, mais également pour tenir compte des exigences de la protection des données, il est nécessaire d'intégrer lesdites

---

65 Relativement au contenu du Règlement, cf. la publication du PFPDT intitulée « Que doit contenir un règlement de traitement ? », disponible à cette adresse : https://www.edoeb.admin.ch/datenschutz/00628/00629/00636/index.html?lang=fr&download=NHzLpZeg7t,lnp6I0NTU042l2Z6ln1ae2IZn4Z2qZpnO2Yuq2Z6gpJCDdH9_gmym162epYbg2c_JjKbNoKSn6A--.

66 Notamment en cas de modification du corpus juridique topique.

67 Cette exigence découle directement du principe de l'exactitude des données énoncé à l'art. 5 LPD.

68 Au sens de l'art. 16 LPD.

69 Lorsque le traitement des données est automatisé, les organes fédéraux responsables collaborent avec les l'Unité de stratégie informatique de la Confédération (USIC) ; cette unité s'appelle désormais l'Unité de pilotage informatique de la Confédération, cf. https://www.isb.admin.ch/isb/fr/home.html.

70 Cf. art. 8 à 10 OLPD.

exigences dès les premières phases de développement d'un projet informatique. Ainsi, l'article 20 OLPD prévoit une obligation pour les organes fédéraux de soumettre à leur conseiller à la protection des données au sens de l'article 11a LPD tous leurs projets de traitement automatisé de données personnelles dès le début de leur développement (art. 20 al. 2 OLPD). À défaut d'un tel conseiller, le projet doit être transmis au préposé. L'annonce au préposé se fait par l'entremise de l'UPIC lorsque les projets doivent également lui être annoncés. Pour les autres projets, l'annonce se fait directement au préposé fédéral[71].

Afin d'éviter des doubles emplois et des actions en ordre dispersé, l'article 20 alinéa 3 prévoit une collaboration entre le préposé et l'UPIC dans l'examen et le contrôle des mesures techniques nécessaires à garantir la protection des données. En particulier, le préposé prend l'avis *de l'UPIC* avant d'émettre une recommandation.

Parmi les mesures techniques et organisationnelles, l'article 21 prévoit l'adoption de règlements de traitement pour les fichiers fédéraux automatisés qui contiennent des données sensibles, qui sont utilisées par plusieurs organes fédéraux ou qui sont rendues accessibles aux cantons[72], à des autorités étrangères, à des organisations internationales ou à des personnes privées.

Le règlement de traitement doit être conçu comme une documentation gérée par l'organe responsable qui donne des informations sur son organisation interne et celle des organes ou personnes participant au fichier. Il donne des informations sur l'organisation et la structure dans laquelle se situe le fichier ou le système de traitement automatisé, ainsi que des informations sur l'accomplissement par les utilisateurs de leurs tâches dans le temps et dans l'espace. Le Règlement doit en particulier décrire les procédures de traitements des données, les procédures de contrôle, le déroulement des principales opérations de traitement. Il documente sur l'élaboration et la gestion du fichier[73].

Un tel règlement doit contenir les informations nécessaires à l'annonce du fichier conformément à l'article 16 OLPD. Ces informations doivent être complétées par des informations sur la source des données[74], sur les finalités pour lesquelles les données sont régulièrement communiquées ou échangées, sur les procédures de contrôle et plus précisément sur les mesures techniques et organisationnelles, y compris la réglementation des accès des différents utilisateurs, la description des champs de données et leur

---

71 Commentaire de l'Office fédéral de la justice (OFJ) à l'appui de l'ordonnance du 14 juin 1993 relative à la loi fédérale sur la protection des données, p. 11, étant précisé que ce commentaire peut être consulté à cette adresse : https://www.edoeb.admin.ch/org/00129/index.html?lang=fr&download.

72 Comme par exemple le système RIPOL, soit le système de recherches informatisée de police : https://www.admin.ch/opc/fr/classified-compilation/20161966/index.html.

73 Présentation des diverses fonctions du système ou du fichier, périodicité des traitements.

74 Il sera également possible d'y indiquer la procédure de collecte des données et la manière de les saisir.

rattachement aux différentes unités d'organisation et d'exécution[75], les procédures de traitement des données et notamment la procédure à suivre lorsque la personne concernée fait usage de son droit d'interdire une communication ou un traitement de données, la durée de conservation des données personnelles et la procédure d'anonymisation, d'archivage ou de destruction des données, ainsi que sur la configuration des moyens informatiques utilisés pour l'accomplissement des tâches[76]. Le règlement doit finalement préciser la procédure d'exercice du droit d'accès des personnes concernées et indiquer l'organe ou la personne responsable de la protection et de la sécurité des données.

La LPD règle expressément le traitement sur mandat effectué ou confié par des organes fédéraux à l'article 10a LPD. L'article 36 4e alinéa lettre b LPD confère au Conseil fédéral la compétence de préciser les conditions d'un tel traitement. Ainsi aux termes de l'article 22 OLPD, lors du traitement par un tiers, l'organe fédéral qui fait traiter des données personnelles demeure responsable de la protection des données. Cela implique pour lui l'obligation de veiller à ce que le traitement s'effectue conformément au mandat et que le mandataire ne traite les données que pour l'exécution du mandat. Il doit également assurer l'exercice du droit d'accès. En règle générale, l'octroi d'un mandat devrait faire l'objet d'un contrat écrit entre l'organe fédéral et le tiers mandaté lorsque celui-ci n'est pas lui- même un organe fédéral. Un tel contrat devra en tous les cas être conclu lorsque le mandataire n'est pas soumis à la LPD ou à des dispositions légales offrant une protection équivalente. Entre organes fédéraux, l'octroi de mandat devrait faire l'objet d'un document écrit[77].

Après prise de connaissance de ces normes techniques et organisationnelles de la protection des données censées concrétiser le principe de la sécurité des données, chacun conviendra du fait que les normes figurant dans la LPD et l'OLPD sont totalement insuffisantes pour permettre à un néophyte de respecter les exigences légales. Ainsi que le mettent en exergue les spécialistes[78], une solution globale doit être envisagée, laquelle tiendra compte tant de la sécurité IT que de la sécurité physique, ainsi que des documents enregistrés sous forme électronique et sous forme physique. Il s'agit donc d'une tâche complexe et protéiforme.

---

75 En particulier les accès des utilisateurs, la nature et l'étendue de ces accès par rapport aux tâches à accomplir.

76 Informations techniques sur les installations, notamment emplacement des terminaux, description des supports de données et du mode de communication des données, les réseaux, ainsi que les matériels et les logiciels utilisés.

77 Commentaire de l'Office fédéral de la justice (OFJ) à l'appui de l'ordonnance du 14 juin 1993 relative à la loi fédérale sur la protection des données, p. 11, étant précisé que ce commentaire peut être consulté à cette adresse : https://www.edoeb.admin.ch/org/00129/index.html?lang=fr&download.

78 WINKLER, p. 113.

La loi renferme également deux normes incitatives, dont l'objectif est d'améliorer l'effectivité de la protection des données. Ces normes sont intéressantes en ce sens qu'elles permettent de simplifier la résolution de l'équation de la compliance en matière de protection des données.

Il s'agit de la certification[79] et du recours à un conseiller à la protection des données indépendant[80].

Le Conseiller interne à la protection des données se chargera de la mise en œuvre interne et du respect des dispositions de la législation applicable, ce qui permet d'échapper à l'obligation d'annonce des fichiers. Cette libération du devoir d'annonce suppose toutefois que la personne choisie soit au bénéfice de connaissances spécialisées nécessaires et qu'elle puisse exercer son activité en totale indépendance.

La certification a été rendue obligatoire dans le cadre de l'assurance-maladie obligatoire pour les services de réception des données des assureurs maladie pour les factures *Diagnoses Related Groups*[81] (DRG)[82]. Elle fait l'objet de l'ordonnance sur les certifications en matière de protection des données du 28 septembre 2007[83]. Cette certification, qui est du ressort d'organismes privés, a pour but d'améliorer la protection et la sécurité des données. Conformément à l'article 4 al. 3 OCPD, le PFPDT émet les directives sur les exigences minimales qu'un système de gestion de la protection des données doit remplir[84]. En sus des exigences formulées par l'OCPD, il convient de documenter les processus dans le cadre de la protection des données pour obtenir la certification. L'ampleur de la tâche ne doit ainsi pas être sous-estimée.

---

79 Cf. art. 11 en relation avec l'art. 11a al. 5 let. f LPD.

80 Cf. art. 11a al. 5 let. e LPD.

81 Pour une présentation du SwissDRG : http://www.swissdrg.org/fr/index.asp?navid=0&fileSsi=/de/index.asp et de plus amples informations relativement à la certification : https://www.edoeb.admin.ch/datenschutz/00756/00973/index.html?lang=fr.

82 WALTER p. 119.

83 OCPD, RS 235.13.

84 Ces informations sont accessibles ici : https://www.edoeb.admin.ch/datenschutz/00756/00974/index.html?lang=fr.

D. Le guide relatif aux mesures techniques et organisationnelles de la protection des données publié par le Préposé fédéral

Le Préposé a édicté en août 2015 un guide[85], dont le but est de permettre une introduction aux risques liés à la protection des données dans les systèmes d'information actuels. Il a été conçu comme une aide à la mise en œuvre de mesures adéquates. Ce guide est avant tout destiné aux personnes en charge des systèmes d'information, techniciens ou non et qui sont confrontés directement au problème de la gestion des données personnelles[86].

Il est organisé en quatre thématiques : l'accès aux données, le cycle de vie des données, le transfert des données et le droit d'accès aux données. Pour chaque thématique, différents points auxquels il faut veiller sont mis en exergue. Des mesures sont proposées y relativement, mesures qui constituent des lignes directrices générales et doivent faire l'objet d'une adaptation aux spécificités des projets et organisations. Il s'agit donc de bonnes pratiques qui doivent faire l'objet d'une analyse contextuelle et qui ne sauraient suppléer à un examen attentif des spécificités de chaque cas[87].

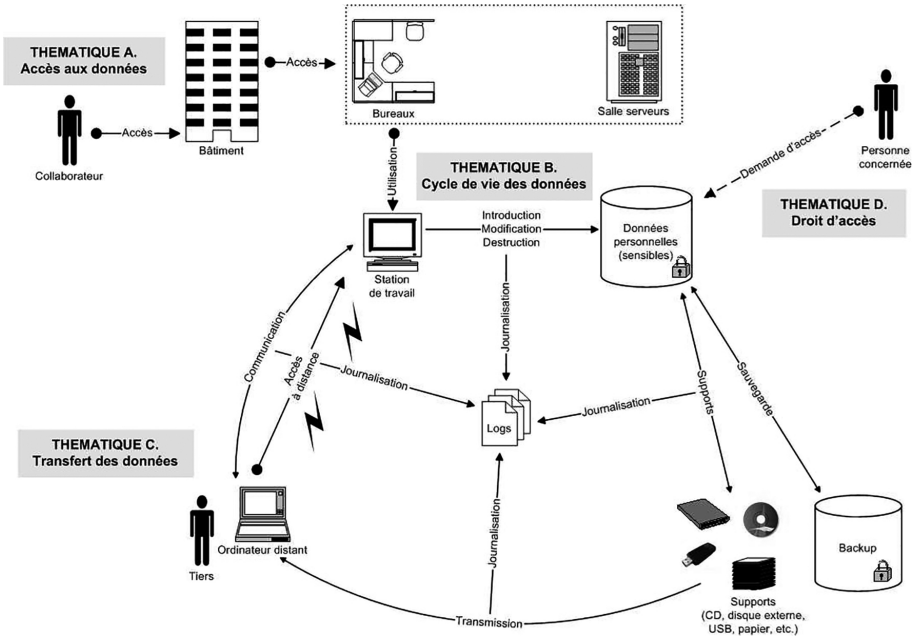
Voici la vue d'ensemble de l'application des mesures techniques et organisationnelles, chaque partie étant commentée par thématique dans les différents chapitres du guide :

---

85 Le guide est accessible à cette adresse : https://www.edoeb.admin.ch/datenschutz/00628/00629/00636/index.html?lang=fr.

86 Préposé fédéral à la protection des données et à la transparence, Guide relatif aux mesures techniques et organisationnelles de la protection des données, août 2015, p. 3.

87 A l'aune notamment de la sensibilité des données, de la nature des traitements, de l'étude de l'information utilisée, etc.



Ce guide a fait l'objet d'une révision terminologique[88] lors d'une récente actualisation. Partant des définitions légales ou des niveaux de risque associé à leur traitement, les données personnelles ont été classées en fonction de leur nature[89] : données « non sensibles », « sensibles » et « ultrasensibles ». En termes de niveaux de risque, les données sensibles et les profils de la personnalité au sens de la loi fédérale sur la protection des données (art. 3 let. c et d LPD) appartiennent au niveau de risque « élevé » (classe « sensible »), tandis que les données personnelles non sensibles recouvrent les niveaux de risque « moyen » et « minimal » (classe « non sensible »). Le niveau de risque « très élevé » (classe « ultrasensible ») est quant à lui réservé aux données dont l'abus peut mettre en danger la vie ou l'intégrité corporelle des personnes concernées[90].

---

88 Rapport d'activité du Préposé fédéral à la protection des données et à la transparence, n° 23 (2015/2016), p. 17.

89 Cette classification ne doit pas être confondue avec celle de la protection de l'information (INTERNE/CONFIDENTIEL/SECRET), qui vise elle à protéger les intérêts nationaux conformément à l'Ordonnance concernant la protection des informations de la Confédération du 4 juillet 2007 (OPrl, RS 510.411).

90 Rapport d'activité du Préposé fédéral à la protection des données et à la transparence, n° 23 (2015/2016), p. 17 ; les deux types de classification présentent des similitudes, de sorte que le PFPDT conseille une mise en parallèle des mesures techniques et organisationnelles de protection associées à

À partir de la classe « sensible »[91], un chiffrement des transmissions et des mémorisations est obligatoire et ce quel que soit le système de gestion de données.

Il convient de relever que l'exigence de classification des données/informations fait partie intégrante de la majorité des standards internationaux de sécurité des informations/ données[92].

E. Le guide pour le traitement des données personnelles dans le secteur du travail (traitement par des personnes privées), émis par le Préposé fédéral[93]

Ce guide[94] qui s'adresse tant aux employés qu'aux employeurs répond aux questions suivantes :

- Quelles données l'employeur est-il autorisé à traiter ?
- Comment doit-il procéder ?
- Est-il tenu de renseigner ses employés sur ces traitements de données ?
- Doit-il enregistrer ses fichiers du personnel ?
- Combien de temps les données qu'il traite peuvent-elles être conservées ?

Après un aperçu des principales normes applicables à la protection des données dans les rapports de travail, le guide commente quelques exemples concrets de traitement des données, depuis le dépôt d'une candidature jusqu'à la cessation des rapports de travail, en

chaque niveau de classification (non sensible/INTERNE, sensible/CONFIDENTIEL, ultrasensible/ SECRET), car cela permet de gagner en simplicité, efficacité et clarté.

91 Respectivement confidentiel.

92 A titre exemplatif, citons la mesure A8.2 (Classification de l'information) de la norme ISO/CEI 27001 : 2013.

93 Il existe d'autres guides qui méritent l'attention dans le domaine du droit du travail, mais il est renoncé à les évoquer ici par souci de synthétisation : Guide relatif aux systèmes de reconnaissance biométrique, Droits de la personne concernée en matière de traitement des données personnelles, Guides relatifs à la surveillance de l'utilisation d'Internet et du courrier électronique au lieu de travail (économie privée et administration fédérale), Guide pour le traitement des données personnelles dans le secteur privé, Guide pour le traitement des données personnelles dans l'administration fédérale, etc., étant précisé que tous sont accessibles ici : https://www.edoeb.admin.ch/datenschutz/00628/00629/ index.html?lang=fr.

94 Le guide est accessible à cette adresse : https://www.edoeb.admin.ch/datenschutz/00628/00629/00633/ index.html?lang=fr.

passant par l'engagement. Enfin, il examine la question de l'utilisation des systèmes de contrôle ou de surveillance des postes de travail[95].

Le guide fourmille d'exemples et constitue une première approche intéressante qui ne dispense toutefois pas le lecteur de consulter d'autres sources, dont la jurisprudence abondante en cette matière[96].

F. Le droit cantonal : l'exemple de la loi valaisanne sur l'information du public, la protection des données et l'archivage

Les traitements de données effectués par les organes cantonaux ou communaux sont réglés par les législations cantonales et sont ainsi de la compétence des préposés cantonaux et communaux à la protection des données[97]. Le PFPDT est quant à lui compétent pour les traitements de données effectués par des organes fédéraux et par des personnes privées.

Dans le canton du Valais, la protection des données informatiques est réglée, s'agissant des autorités[98], par la loi sur l'information du public, la protection des données et l'archivage du 9 octobre 2008[99]. Il convient également de mentionner le Règlement d'exécution de la loi sur l'information du public, la protection des données et l'archivage[100]. La dichotomie est donc similaire à celle prévalant sur le plan fédéral, où l'on opère un distinguo entre le secteur privé et le secteur public.

Les mesures techniques et organisationnelles à respecter figurent aux articles 28 et suivant RèLIPDA. Il s'agit en réalité d'une concrétisation du principe de sécurité des données prévu à l'article 21 LIPDA, qui rappelle aux autorités qu'elles doivent prendre toutes les mesures appropriées organisationnelles et techniques pour protéger les données en leur possession contre certains risques comme la falsification, le vol, la perte ou tout traitement illicite. Celles-ci assurent en premier lieu la sécurité de l'information, notamment sa

---

95 Deux guides topiques sont consacrés à cette thématique : Guide relatif à la surveillance de l'utilisation d'Internet et du courrier électronique au lieu de travail (économie privée) et Guide relatif à la surveillance de l'utilisation d'Internet et du courrier électronique au lieu de travail (administration fédérale), accessible à cette adresse : https://www.edoeb.admin.ch/datenschutz/00763/00983/00988/index.html?lang=fr.

96 DUNAND, pp. 56 ss ; MÉTILLE, La surveillance électronique, pp. 99 ss.

97 https://www.edoeb.admin.ch/org/00146/00147/index.html?lang=fr.

98 La notion d'autorités est définie à l'article 3 al. 1 de la loi ; pour de plus amples informations, cf. FANTI, La notion de document officiel, p. 411.

99 LIPDA, RS/VS 170.2.

100 RèLIPDA, RS/VS 170.200.

confidentialité, sa disponibilité et son intégrité. Des garanties de sécurité suffisantes sont particulièrement importantes dans le cadre de la vidéosurveillance[101].

Les mesures générales sont prévues à l'article 28 RèLIPDA, alors que les mesures particulières, soit celles relatives aux traitements automatisés de données personnelles, sont régies à l'article 29 RèLIPDA. À cela s'ajoute un article topique en matière de journalisation (art. 30) qui assure une protection complémentaire en cas de nécessité, soit lorsque les mesures préventives ne suffisent pas à garantir la protection des données. Il s'agit évidemment de principes généraux qui nécessitent une concrétisation.

Fondamentalement, les exigences ne diffèrent pas de celles figurant dans la LPD et l'OLPD qui pourront donc favoriser une application analogique et similaire des grands principes de la sécurité des données.

G. Casuistique[102]

– **Envoi de certificats de caisse de pension**[103] : les certificats doivent être remis de telle sorte que seule la personne assurée à l'exclusion de tout tiers, notamment l'employeur, puisse prendre connaissance de leur contenu ; le PFPDT ayant appris qu'AXA Fondation de prévoyance professionnelle Winterthur transmettait les certificats de prévoyance par le biais de l'employeur avec la seule mention « confidentielle », il a émis une recommandation qui n'a pas été suivie par AXA[104] ; le Tribunal administratif fédéral s'est prononcé dans cette affaire le 10 avril 2012[105] et il a suivi la recommandation du PFPDT en considérant que la mention « confidentielle » ne protégeait pas contre la copie ou la prise de connaissance par l'employeur. Dans l'hypothèse où AXA souhaite transmettre les certificats par le biais de l'employeur, elle doit s'assurer de la confidentialité par exemple en utilisant des enveloppes individuelles fermées. Il s'agit de mesures simples à mettre en place et n'engendrant pas de coûts disproportionnés[106].

---

101 Message accompagnant le projet de loi sur l'information du public, la protection des données et l'archivage (LIPDA), p. 10.

102 Il s'agit d'un choix subjectif visant à illustrer le propos.

103 Rapport d'activité du Préposé fédéral à la protection des données et à la transparence, n° 21 (2013/2014), p. 57.

104 Le Préposé a conséquemment sollicité du Département fédéral de l'Intérieur (DFI) de rendre une décision ordonnant à AXA de se conformer à sa recommandation. Le DFI n'a toutefois pas suivi l'avis du Préposé dans sa décision, Préposé qui a donc saisi le Tribunal administratif fédéral.

105 ATAF 2012/14 ; cf. également FUHRER, pp. 298 ss et MÉTILLE, pp. 117 et 118.

106 Ainsi que le relève le PFPDT dans son Rapport d'activité n° 21 (2013/2014) (pp. 57 et 58), la notion de tiers a été centrale pour la résolution du problème. Il s'agit d'une notion qui ne figure pas dans la

- **Obligation d'informer l'employeur dès l'apparition des premiers signes de maladie**[107] : Le Département fédéral des finances reprochait à l'une de ses employées de ne pas l'avoir informé suffisamment tôt de son état de santé et de son incapacité de travail[108] ; selon le TAF un ou une employé(e) a l'obligation d'informer son employeur à temps d'absences ou d'incapacités de travail prévisibles[109] ; son devoir de fidélité[110] ne lui impose toutefois pas d'informer son employeur de l'apparition d'une maladie ; la seule exception est celle où la protection des parties ou des tiers l'exige[111].
- **Vidéosurveillance dans des établissements de restauration**[112] : les enregistrements vidéo pouvant entraîner une surveillance systématique des comportements sont, selon l'ordonnance relative à la loi sur le travail[113], illicites ; les sanctions en cas de violation de cette ordonnance étant de la compétence des inspections cantonales du travail, le PFPDT renvoie les personnes concernées à agir auprès de ces autorités.
- **Questionnaire de santé lors d'une candidature**[114] : l'admissibilité d'un tel questionnaire dépend du poste ou de la fonction convoitée ; si un candidat doit remplir un questionnaire, il doit certes indiquer ses pathologies (par exemple diabète), mais le médecin ne peut communiquer aucun diagnostic à l'employeur ; il ne peut que l'informer d'une adéquation insuffisante pour le poste concernée, par exemple si la maladie compromet directement et actuellement la capacité de travail ou empêche la réalisation des tâches prévues.
- **Renseignements fournis par de précédents employeurs dans le cadre d'une postulation**[115] : un employeur ne doit demander ou transmettre que les informations

---

LPD. Selon cette jurisprudence, un tiers est toute personne qui, du point de vue de la nature de ses attributions au sein d'une entreprise, ne nécessite pas l'accès aux données personnelles en jeu pour accomplir ses tâches. En l'occurrence, l'employeur n'a pas à accéder à ces données qui sont susceptibles d'avoir une portée stratégique, dès lors qu'elles renseignent notamment sur un divorce ou encore l'acquisition de la propriété ou une incapacité de travail temporaire.

107 TAF A-531/2014 du 17 septembre 2014.

108 FLUECKIGER/DAHMEN, p. 139.

109 En vertu de l'art. 20 de la loi sur le personnel de la Confédération (LPers) du 24 mars 2000, RS 172.220.1.

110 Prévu à l'art. 20 LPers.

111 Par exemple en cas de maladie contagieuse.

112 Rapport d'activité du Préposé fédéral à la protection des données et à la transparence, n° 22 (2014/2015), p. 54.

113 Cf. art. 26 (surveillance des travailleurs) de l'Ordonnance 3 relative à la loi sur le travail (OLT 3) du 18 août 1993, RS 822.113.

114 Rapport d'activité du Préposé fédéral à la protection des données et à la transparence, n° 22 (2014/2015), p. 54.

115 Rapport d'activité du Préposé fédéral à la protection des données et à la transparence, n° 22 (2014/2015), p. 57.

pertinentes dans la perspective du futur poste ou nécessaires à la mise en œuvre du contrat de travail ; s'agissant de relater les traits essentiels de la personnalité du travail, il s'agit de profils de personnalité qui nécessitent le consentement préalable et explicite du travailleur ; ce consentement ne saurait être déduit de la communication de la liste des précédents employeurs, mais peut être inféré de la mention d'un ancien employeur ou d'un ancien supérieur à la rubrique « Références » ; il appartient à l'ancien employeur de s'assurer de l'existence du consentement et d'informer le candidat de la communication de renseignements et de leur teneur ; l'octroi de renseignements non autorisés constitue une atteinte illicite à la personnalité qui peut faire l'objet d'une action civile en application de l'article 15 LPD ; le candidat peut également agir sur le plan pénal (art. 35 LPD) et engager des poursuites pénales contre son ancien employeur qui aurait communiqué des données sensibles ou un profil de personnalité sans son consentement.

– **Transmission de données dans le domaine des mesures d'accompagnement de la loi sur les travailleurs détachés**[116] : les données personnelles des collaborateurs des sous-traitants peuvent être transmises en cas de responsabilité solidaire ou de contrôles prévus par la loi sur les travailleurs détachés[117] ; toutefois, le principe de proportionnalité doit toujours être respecté, ce qui signifie que seules les données nécessaires à la réalisation de l'objectif prévu peuvent être transmises.
– **Contrôle de sécurité relatif aux collaborateurs dans le domaine privé**[118] : suite à diverses requêtes, le PFPDT a clarifié les exigences en matière de contrôle de sécurité[119] ; dans les secteurs de l'informatique, des banques et des technologies de pointe, le personnel a accès à des installations et des données sensibles ; les entreprises sont autorisées à soumettre à un contrôle de sécurité les collaborateurs qui présentent un risque conséquent du fait de leur activité ; une analyse interne des risques doit déterminer la nature et l'ampleur du contrôle de sécurité ; l'article 328b du Code des

[116] Rapport d'activité du Préposé fédéral à la protection des données et à la transparence, n° 22 (2014/2015), p. 58.
[117] Loi fédérale sur les mesures d'accompagnement applicables aux travailleurs détachés et aux contrôles des salaires minimaux prévus par les contrats-types de travail du 8 octobre 1999, RS 823.20.
[118] Rapport d'activité du Préposé fédéral à la protection des données et à la transparence, n° 23 (2015/2016), p. 49.
[119] Les explications formulées sont accessibles à la page suivante : https://www.edoeb.admin.ch/datenschutz/00763/00975/01240/index.html?lang=fr.

obligations[120] trouve application[121] et détermine ce qui est admissible[122] ; si des collaborateurs se voient confier une tâche dans un domaine à risque, l'employeur est en droit de réaliser un contrôle de sécurité ; il a toutefois un devoir d'assistance vis-à-vis de son personnel, ce qui signifie qu'il doit limiter sa collecte de données à ce qui est absolument nécessaire[123] ; l'employé doit être informé[124] préalablement au contrôle de sécurité et par écrit[125] relativement à l'objectif de la collecte d'informations et à la durée de conservation des données ; l'employeur devra motiver la nécessité du contrôle dans chaque cas particulier et lui indiquer qui va diligenter les démarches[126] ; idéalement le contrôle doit être opéré au début du rapport de travail, mais parfois les circonstances peuvent le rendre nécessaire une fois le rapport établi[127], auquel cas la mesure doit être annoncée suffisamment tôt pour que le collaborateur puisse y réfléchir[128] ; il est vivement conseillé au collaborateur qui refuserait le contrôle de

---

120 Dont le libellé est le suivant : *L'employeur ne peut traiter des données concernant le travailleur que dans la mesure où ces données portent sur les aptitudes du travailleur à remplir son emploi ou sont nécessaires à l'exécution du contrat de travail. En outre, les dispositions de la loi fédérale du 19 juin 1992 sur la protection des données sont applicables.*

121 Dans certains secteurs économiques comme le domaine bancaire, des règles spécifiques ont été édictées, à l'instar des circulaires de l'Autorité fédérale de surveillance des marchés financiers (FINMA).

122 Un extrait du casier judiciaire peut par exemple être sollicité pour les personnes qui sont en contact quotidiennement avec de grandes quantités d'argent, mais s'agissant de données sensibles, l'employeur devra appliquer les principes de la protection des données avec la plus grande rigueur.

123 Ces principes s'appliquent également à l'employeur chargé du contrôle des personnes sur la base d'un contrat. L'employeur doit s'assurer que l'étendue du contrôle demandé obéit au contrôle de proportionnalité.

124 Les vérifications secrètes sont illicites.

125 Une mention par oral suffit dans un premier temps dans le cas d'un entretien avec un candidat postulant pour un emploi nécessitant un contrôle.

126 Spécifiquement si le contrôle est opéré par une société externe ou qu'il a lieu à l'étranger. Dans une telle hypothèse, en vertu de l'art. 10a LPD, la responsabilité du traitement incombe toujours à l'employeur et il faut que seuls les traitements qu'il serait en droit de diligenter lui-même soient effectués.

127 En pratiques, notamment dans le secteur bancaire, le contrôle est réitéré de manière régulière, chaque 5 ans par exemple.

128 En cas de refus injustifié de la part du salarié celui-ci devra en assumer les conséquences sur le plan du droit du travail, ce qui signifie qu'il peut voir son contrat résilié à tout le moins ordinairement dès lors que l'adéquation avec les risques mis en exergue ne peut être évaluée et qu'il n'existe pas de possibilité d'exercer dans l'entreprise d'autres tâches ne nécessitant pas de contrôle de sécurité. Autre est la question d'un licenciement avec effet immédiat dans l'hypothèse d'un refus injustifié. Celui-ci pourrait entrer en ligne de compte si l'employeur est soumis à un cadre réglementaire qui lui impose le respect en temps réel de condition d'exercice de l'activité, respectivement qui le frappe en cas d'inaction de sanctions telle que le retrait de l'autorisation de pratiquer.

sécurité en raison du fait que celui-ci est disproportionné[129] ou non indispensable pour son activité d'en parler à son employeur et de solliciter de savoir pourquoi il doit fournir les informations ; finalement en application de l'article 8 LPD, un collaborateur peut solliciter en tout temps d'accéder aux données, respectivement aux documents destinés au contrôle de sécurité[130].

H. Windows 10

Le système d'exploitation Microsoft Windows 10 mérite une attention particulière. Dans son 23e rapport[131], le PFPDT indiquait avoir étudié en détail le traitement des données opéré et constaté que, lors du processus d'installation, les « paramètres express » proposés aux utilisateurs dans la fenêtre de démarrage rapide activaient pas défaut presque tous les transferts de données et les accès s'y rapportant[132]. Conséquemment, soit sur la base de ce constat, le PFPDT a engagé en août 2015 une procédure d'établissement des faits et adressé à Microsoft un questionnaire sur les traitements de données liés à ce système d'exploitation. Le but de la démarche entreprise était de déterminer le type et l'étendue des données transmises et de savoir si les utilisateurs avaient été informés de manière suffisamment claire, respectivement si leur consentement avait été obtenu de manière licite.

Par communiqué du 11 janvier 2017[133], le PFPDT indiquait avoir terminé l'établissement des faits concernant ce système d'exploitation : « *Les clarifications du PFPDT ont montré que le traitement des données dans le cadre du système d'exploitation Windows 10 n'était pas entièrement conforme au principe de la protection des données. La structure et le contenu des pages "démarrer rapidement" et "paramètres de personnalisation" ne répondaient que partiellement aux exigences de la transparence de l'information. En effet, des informations quant à la durée de conservation des données transmises ainsi qu'au contenu des données de navigation, diagnostic et rapports d'erreur manquaient. De plus, il était difficile pour l'utilisateur d'obtenir davantage d'informations sur les traitements*

129 La proportionnalité doit faire l'objet d'un examen *in concreto.* En cas de litige, il convient de saisir la justice civile, le PFPDT n'étant pas en mesure de traiter des dossiers individuels.

130 Il convient de préciser que les données qui ne sont plus utiles et/ou nécessaires doivent être détruites, respectivement qu'elles ne peuvent être réutilisées à d'autres fins.

131 Rapport d'activité du Préposé fédéral à la protection des données et à la transparence, n° 23 (2015/2016), p. 29.

132 Sont ainsi transmis à Microsoft des données de localisation, les réseaux WLAN reconnus dans l'environnement des utilisateurs de Windows 10, les historiques de navigation et de recherche, les entrées vocales, les entrées de dessin à main levée et au clavier, ainsi que des données de feedback et de diagnostic.

133 https://www.edoeb.admin.ch/aktuell/01437/index.html?lang=fr.

spécifiques des données, par exemple en consultant des passages précis de la déclaration de confidentialité. ». Suite à ce constat de violation de la LPD, Microsoft a soumis différentes propositions visant à remédier aux insuffisances mises en exergue. Après discussion, les parties sont parvenues à un accord quant aux adaptations à diligenter, lesquelles permettront de donner des indications plus précises sur le traitement de données. Selon le PFPDT, « *grâce aux nouvelles pages de configuration qui s'afficheront lors du processus d'installation, les utilisateurs seront rendus attentifs au fait qu'ils devront définir dans quelle mesure les données seront traitées et transmises, et ensuite l'autoriser* ».

La mise en œuvre technique des adaptations sollicitées interviendra, à l'échelle mondiale, pour les deux nouvelles mises à jour du logiciel Windows 10, prévues en 2017[134]. Indépendamment de l'adaptation des futures procédures d'installation convenue entre les parties, les utilisateurs de Windows 10 ont toujours la possibilité – dans les paramètres du système – d'adapter le traitement et la transmission qui sont faits de leurs données[135].

Le PFPDT estime que la solution convenue avec Microsoft, particulièrement concernant le lien direct aux passages pertinents de la déclaration de confidentialité ainsi que les possibilités de configuration lors de l'installation, constitue un standard minimum auquel devront dorénavant se conformer les autres entreprises[136].

Les recommandations du PFPDT portant sur l'amélioration de la transparence dans le traitement des données ainsi que sur les choix d'installation s'y rapportant ayant été acceptées par Microsoft, une décision judiciaire ne s'avère pas nécessaire.

---

[134] Suite à la première mise à jour, lors de la réinstallation du logiciel respectivement de la mise à jour du système d'exploitation, les options de configuration concernant la transmission de données seront, au moyen d'informations détaillées, indiquées à tous les utilisateurs. Après la deuxième mise à jour, ces derniers pourront, lors de l'installation, accéder directement aux passages correspondants dans la déclaration de confidentialité la plus actuelle. Ce procédé gagne, selon le PFPDT, en transparence et permettra aux utilisateurs de trouver plus facilement les informations pertinentes dans la déclaration de confidentialité.

[135] Un aperçu de la nouvelle page de configuration de Windows 10 est disponible sur le blog de Microsoft : https://blogs.windows.com/windowsexperience/2017/01/10/continuing-commitment-privacy-windows-10/#48qc3Y0ykqGYARM2.97.

[136] Le PFPDT indique à cet égard qu'au cours de prochaines procédures d'établissement des faits, il se basera sur cette solution pour l'examen du traitement des données. Il s'agit donc d'un standard que les autres entreprises soumises à son pouvoir de régulation devront adopter rapidement.

À titre de comparaison, la Commission Nationale de l'Informatique et des Libertés[137] a mis publiquement[138] en demeure[139] Microsoft Corporation de cesser la collecte excessive de données et le suivi de la navigation des utilisateurs sans leur consentement[140]. La CNIL lui a également demandé d'assurer de manière satisfaisante la sécurité et la confidentialité des données des utilisateurs. Elle a effectué 7 contrôles en ligne en avril et juin 2016 et interrogé la firme sur certains points exposés dans sa politique de confidentialité pour vérifier la conformité de Windows 10 avec les normes légales. Les vérifications ont mis en exergue de nombreux manquements[141]. Microsoft a donc été mise en demeure de se conformer à la loi dans un délai de 3 mois. Le but de la démarche était, selon la CNIL, de permettre aux utilisateurs d'exercer leur choix librement en étant correctement informés de leurs droits. Une demande de prolongation de 3 mois formulée par la firme[142] ayant été acceptée par la CNIL, nous saurons prochainement qu'elles sont les intentions de Microsoft, et il sera alors possible de comparer les résultats obtenus par les différents régulateurs, étant d'emblée précisé que les corpus juridiques se distinguent notablement.

Si Microsoft devait ne pas se conformer à la mise en demeure dans le délai imparti, la Présidente de la CNIL pourra désigner un rapporteur qui, cas échéant, pourra établir un rapport proposant à la formation restreinte de la CNIL, chargée de sanctionner les manquements à la loi, de prononcer une sanction à l'égard de la société.

I. Quelques exemples d'utilisation des moyens techniques en vue d'une amélioration de la protection des données

Ainsi que le mentionne opportunément le Professeur JEAN-HENRY MORIN[143], il existe différents moyens techniques destinés à la gestion des risques, respectivement à faciliter technologiquement le respect des normes en matière de protection des données.

---

137 Abrégée ci-après CNIL : https://www.cnil.fr/professionnel.

138 La mise en demeure a été rendue publique notamment en raison de la gravité des manquements constatés et du nombre de personnes concernées (plus de 10 millions d'utilisateurs Windows 10 en France) ; la décision de rendre publique la mise en demeure peut être consultée ici : https://www.cnil.fr/sites/default/files/atoms/files/2006-185_publicite_med_microsoft.pdf.

139 La décision est accessible à cette adresse : https://www.cnil.fr/sites/default/files/atoms/files/2016-058-med_microsoft_corporation.pdf.

140 https://www.cnil.fr/fr/windows-10-la-cnil-met-publiquement-en-demeure-microsoft-corporation-de-se-conformer-dans-un-delai.

141 Données collectées non pertinentes ou excessives, défaut de sécurité, absence de consentement des personnes, etc.

142 Le délai viendra à échéance le 20 janvier 2017.

143 MORIN, pp. 1-12.

À titre exemplatif, il convient d'évoquer les techniques DLP (Data Loss Prevention)[144] qui constituent des techniques de détection d'« *extrusion* » et ont été développées aux fins de permettre de prévenir la fuite d'information[145]. Ces techniques sont très utilisées dans les organisations, dont les banques. Avec la prochaine mise en vigueur[146] de la Circulaire 2008/21 révisée de la FINMA relative aux risques opérationnels des banques[147] (intitulée « Exigences de fonds propres et exigences relatives aux risques opérationnels dans le secteur bancaire), les banques se sont littéralement précipitées sur ces outils pour éviter que certaines données ne fuitent et que l'accès et/ou la transmission de données sensibles effectués sans autorisation soient détectés et bloquées à temps. La circulaire précitée exige[148] en effet que la direction de l'établissement bancaire implémente un concept de gestion des risques en lien avec les cyberrisques, lequel doit couvrir un certain nombre d'aspects[149] et garantir une mise en œuvre appropriée grâce à des processus appropriés, ainsi qu'une définition claire des tâches, rôles et responsabilités. La direction doit ordonner régulièrement des analyses de vulnérabilité et des tests d'intrusion visant à permettre de protéger les données et systèmes IT critiques et/ou sensibles contre les cyberattaques.

Les techniques DLP permettent certes de compenser une partie des problèmes, mais ne sont d'aucune utilité une fois que l'information a quitté le périmètre de l'organisation. Il est nécessaire de compléter ce type de mesures par des technologies permettant la protection persistante du contenu (Technologies DRM). Les DRM (acronymes de *Digital Rights Management*, en français : gestion des droits numériques ou électroniques) constituent des mesures techniques de protection en ce qu'ils permettent d'associer de

---

144 Il s'agit en réalité d'observer les contenus (*sniffing* en anglais) sur la base de mots clés durant tout le cycle de vie de l'information ; pour de plus amples informations, cf. MORIN, p. 8.

145 Pour un aperçu des solutions disponibles sur le marché : https://www.gartner.com/doc/reprints?id=1-2X96R6A&ct=160128&st=sb.

146 Au 1er juillet 2017.

147 La circulaire peut être consultée ici : https://www.finma.ch/fr/documentation/circulaires/#query=risques%20opérationnels&Order=2.

148 Cf. 135.6*.

149 a. identification des risques potentiels de cyberattaques spécifiques à l'établissement, notamment en ce qui concerne les données et systèmes IT critiques et/ou sensibles,
b. protection des processus opérationnels et de l'infrastructure technologique contre les cyberattaques, notamment sous l'angle de la confidentialité, de l'intégrité et de la disponibilité des données et des systèmes IT critiques et/ou sensibles,
c. identification et désignation rapides des cyberattaques sur la base d'un processus de surveillance systématique de l'infrastructure technologique,
d. réaction aux cyberattaques grâce à des mesures immédiates et ciblées et, dans les cas matériels, maintien de l'activité opérationnelle normale en concertation avec le BCM, et
e. garantie d'un rétablissement rapide de la marche normale des affaires après des cyberattaques, grâce à des mesures appropriées.

façon cryptographique des règles d'usage à du contenu numérique, ceci en toute indépendance du type ou du format de ces données. Le contenu est chiffré et les règles d'usage régissent et gouvernent l'usage de ces contenus. La protection est dite persistante, car le contenu est protégé en tout temps où qu'il se trouve[150]. En utilisant les DRM pour tout le contenu sortant du périmètre, on peut assurer à celui-ci une protection persistante nécessaire. Il convient par souci de transparence et d'objectivité de terminer en relevant l'existence de problèmes multiples (interopérabilité[151], absence de flexibilité en termes d'utilisation, etc.), de sorte que ces moyens techniques ne sauraient se substituer à une analyse dynamique, transversale et protéiforme, respectivement à une évaluation fine de la conformité.

III. Les méthodes alternatives

A. Les normes ISO

Les normes de l'organisation internationale de normalisation (ISO[152]) qui réunit 163 pays présentent un grand intérêt en matière de protection des données informatiques. L'organisation a élaboré à ce jour près de 20'000 spécifications de qualité et de sécurité dans des domaines très divers. Elles sont désignées par l'appellation désormais commune *normes ISO.* Même si l'adhésion à ces normes est toujours volontaire, leur respect par des organisations peut être attesté par des organismes accrédités, ce qui a permis à ces normes d'acquérir un haut degré de crédibilité et une reconnaissance quasi universelle[153].

150 Pour de plus amples informations, cf. MORIN, p. 9.

151 http://fr.calameo.com/read/001574234c6812f0a486f.

152 L'ISO (Organisation internationale de normalisation) est une organisation internationale non gouvernementale, indépendante, dont les 163 membres sont les organismes nationaux de normalisation. Par ses membres, l'Organisation réunit des experts qui mettent en commun leurs connaissances pour élaborer des Normes internationales d'application volontaire, fondées sur le consensus, pertinentes pour le marché, soutenant l'innovation et apportant des solutions aux enjeux mondiaux.

153 COTTIER, N 2, p. 268.

B. Les normes ISO applicables en matière de protection des données

Deux normes visent spécifiquement la protection de la vie privée. Il s'agit de la norme ISO/IEC 29100 : 2011[154] (Technologies de l'information - Technique de sécurité - Cadre privé) et ISO/IEC 27018 : 2014[155] (Technologies de l'information – Techniques de sécurité - Code de bonnes pratiques pour la protection des informations personnelles identifiables dans l'information en nuage public)[156].

La norme ISO 29100 approfondit les principes fondamentaux des domaines de la protection des données personnelles et du respect de la vie privée. Après la présentation de diverses méthodes d'anonymisation[157], la norme définit et commente onze principes de protection des données que le responsable du traitement doit s'engager à respecter[158].

Pour la norme ISO 27018 applicable (tant au secteur public qu'au secteur privé), ces principes complètent dans une annexe normative les points de contrôle spécifiques à appliquer par les sous-traitants de services de cloud public. Ces points de contrôle additionnels sont classés selon les onze principes de la norme ISO 29100 dont l'exercice des droits de la personne concernée, la finalité du traitement, la proportionnalité, etc.

L'adoption de la norme ISO 27018 participe au processus de mise en conformité. Outil de corégulation entre les acteurs du cloud et les autorités de contrôles, elle devrait[159] permettre de répondre aux évolutions actuelles du cadre légal et réglementaire européen[160]. C'est quoi qu'il en soit une amélioration des moyens de protection au niveau international[161]. Elle permet également de sécuriser les relations contractuelles entre les sous-traitants fournisseurs de solutions de Cloud et les clients responsables de traitements. Elle devrait

---

154 Abrégée ci-après ISO 29100.

155 Abrégée ci-après ISO 27018.

156 Ces normes peuvent être téléchargées ici : http://standards.iso.org/ittf/PubliclyAvailableStandards/index.html et ici: https://www.iso.org/obp/ui/#iso:std:iso-iec:27018:ed-1:v1:en.

157 *Ad* 4.4.

158 *Ad* 5.2 à 5.12.

159 Trois applications sur quatre ne seraient en effet pas conformes aux nouvelles normes du RGPD, selon une étude sur les services Cloud menée par Netskope : https://blog.oodrive.fr/blog/2016/08/22/rgpd-les-applications-cloud-sont-elles-pretes-pour-2018/.

160 Pour une analyse des implications de la future réglementation européenne sur les contrats cloud, cf. JOSE MEDIO CACHAFEIRO : http://www.eurocloud.fr/implications-de-future-reglementation-europeenne-contrats-cloud/.

161 De l'avis de la Commission européenne, une cohérence entre le futur cadre juridique et ces normes sera essentielle pour assurer une mise en œuvre systématique et pratique des règles de protection des données par les responsables du traitement (Communication de la Commission européenne COM (2010) 609, p. 19).

également susciter une évolution vers des solutions de certification du cloud sur la base de critères de sécurité de l'information et de respect de la vie privée.

Même si ces normes ne constituent pas la panacée, elles doivent servir de facilitateur dans le cadre de complexe, d'implémentation des exigences des normes en matière de protection des données[162].

IV. La protection des données informatiques par l'intelligence artificielle (IA) et ses garde-fous

A. L'état de la technologie et les développements en matière de cybersécurité

Un récent rapport[163] du National Science and Technology Council de l'Executive Office of the President of the United States of America est spécifiquement consacré à l'intelligence artificielle. Intitulé « *Preparing for the future of Artificial Intelligence* », il évoque brièvement l'état de la technologie[164]. Dans le contexte de la protection des données informatiques, l'IA disposerait de superpouvoirs[165]. La reconnaissance automatique permettrait de détecter aisément les fraudes et des algorithmes seraient en cours de développement pour identifier les menaces que les cerveaux humains et les mécanismes de sécurité traditionnels échouent à reconnaître. L'IA serait donc en passe d'analyser en temps réel les comportements de l'utilisateur pour empêcher notamment des accès interdits aux données ou au système. Il serait même question d'accorder une autonomie à ces systèmes qui pourraient ainsi bénéficier de modules d'autoapprentissage visant notamment à s'adapter aux changements de la réglementation. Nous n'en sommes certes pas à un tel niveau de maturité, mais l'IA à son stade actuel permet d'ores et déjà d'entrevoir les possibilités qui vont se matérialiser à brève échéance. Imaginez ne serait-ce que les économies réalisées en termes de personnels et de software. Une telle évolution n'est pas sans risques.

---

162 BONNET.

163 Le rapport est accessible à cette adresse : https://www.whitehouse.gov/sites/default/files/whitehouse_files/microsites/ostp/NSTC/preparing_for_the_future_of_ai.pdf.

164 En pages 7 à 12.

165 HACK.

B. Le drapeau rouge d'Alan Turing

La loi du drapeau rouge a été pensée par le mathématicien britannique Alan Turing[166]. Elle signifie que tout système autonome doit être conçu de manière à ce qu'il soit improbable de le confondre avec autre chose qu'un système autonome[167]. Il lui est donc fait obligation de s'identifier comme préliminairement à chaque interaction avec un agent tiers. La référence à Alan Turing est liée au test que celui-ci avait développé pour qualifier une machine d'intelligente[168].

Plusieurs voix[169] s'élèvent désormais et s'interrogent sur la nécessité d'imposer aux robots et aux intelligences artificielles la nécessité de se signaler pour éviter toute mésentente. La question n'est pas ubuesque. Après tout, le fait d'être l'objet d'une vidéosurveillance au travail ne doit-il pas être signalé au travailleur ?

Il apparaît difficilement acceptable qu'une surveillance en temps réel soit diligentée, fut-elle opérée par une IA. Le principe de proportionnalité serait violé[170]. En effet, pour être proportionnée, une mesure doit être apte à atteindre le but visé nécessaire et demeurer dans un rapport raisonnable entre le résultat recherché et le moyen utilisé. L'équilibre entre la protection de la sphère privée et celle des intérêts de l'employeur ne saurait être respecté en cas de surveillance de ce type par une IA, nonobstant le fait que celle-ci ne serait pas orientée vers une personne en particulier. Il paraît également difficile d'accepter qu'une IA dotée d'une autonomie et d'un module d'autoapprentissage puisse devenir le garant de la protection des données. Ce faisant, il s'agirait plutôt de donner vie à de nouveaux Léviathans dont personne ne sait si, en définitive, ils ne deviendraient pas des collecteurs plus voraces de données que celles qu'ils sont censés protéger. La seule voie possible consisterait à juguler les fonctionnalités d'une intelligence artificielle[171], ce qui paraît antinomique avec sa raison même d'être.

Dans ce contexte la nécessité d'indiquer la présence d'une IA dans des outils logiciels paraît un minima pour éviter que celle-ci ne devienne une technologie pervasive et qu'elle ne prolifère sans réelle possibilité de contrôle. Pour le surplus, à l'ère de la privacité initiale

---

166 Il est le père de l'informatique, le co-inventeur de l'ordinateur et un visionnaire en matière d'intelligence artificielle.

167 Lors des débuts de l'automobile en Angleterre, les premières voitures à moteur devaient être précédées d'un porteur de drapeau rouge pour signaler qu'il s'agissait d'un véhicule motorisé.

168 Pour un exemple récent : https://humanoides.fr/mit-test-de-turing/.

169 MIGNOT.

170 MÉTILLE, La surveillance électronique, p. 116.

171 En implémentant des garde-fous issus des normes à l'instar d'une gradation des mesures de surveillance.

(Privacy by Design ou by Default), on perçoit encore mal comment les IA pourraient prospérer dans le respect du corpus légal.

V. Conclusions et perspectives

Le 11 janvier 2017, le Conseil fédéral a pris connaissance lors de sa séance hebdomadaire de l'établissement d'un nouveau cadre pour le transfert des données personnelles de la Suisse à des entreprises sises aux États-Unis[172]. La Suisse dispose désormais, à l'instar de l'UE, d'un nouveau cadre qui remplace le « *Safe Harbor*[173] », cadre censé améliorer la protection des données personnelles[174]. Intitulé « Bouclier de protection des données Suisse-Etat-Unis (ou *Privacy Shield*) », il devrait permettre aux données personnelles exportées de Suisse vers les États-Unis de bénéficier des mêmes normes que celles provenant de l'Union européenne, un point fondamental pour la sécurité juridique des échanges économiques et en particulier aussi pour le libre échange des données entre la Suisse et l'UE (précisément dans le domaine commercial).

Le PFPDT considère quant à lui[175] que l'implémentation de ce nouveau cadre permet de garantir un niveau de protection adéquat. Il reconnaît, selon les termes du *Privacy Shield*, l'adéquation du niveau de protection des données et il a ajusté sa liste des États assurant un niveau de protection adéquat (art. 7 OLPD). Il accordera toutefois une importance toute particulière à l'évolution des faits dans la pratique et aux développements juridiques concrets, ce qui signifie qu'il se réserve le droit de procéder à des mises à jour de la liste dans le cadre des évaluations annuelles prévues du *Privacy Shield* s'il le juge approprié au vu de l'exécution effective des accords dont il aura connaissance. Son jugement tiendra également compte de la jurisprudence des tribunaux suisses et, le cas échéant, des décisions de justice dans l'UE.

---

172 Le communiqué de presse du Conseil fédéral peut être consulté ici : https://www.admin.ch/gov/fr/accueil/documentation/communiques.msg-id-65210.html ; quant à la prise de position du PFPDT, elle est disponible ici : https://www.edoeb.admin.ch/datenschutz/00626/00753/01405/01406/index.html?lang=fr.

173 Le Safe Harbor a été invalidé par une décision du 6 octobre 2015 dans l'affaire CJUE C-362/14 *Maximillian Schrems c. Data Protection Commissioner* du 6 octobre 2015 ; la présentation des faits est disponible ici : https://www.edoeb.admin.ch/datenschutz/00626/00753/00970/01320/index.html?lang=fr.

174 Le Conseil fédéral cite le renforcement de l'application des principes de protection des données par les entreprises participantes d'une part, et la gestion et le suivi de ce dispositif par les autorités américaines d'autre part.

175 https://www.edoeb.admin.ch/datenschutz/00626/00753/01405/01406/index.html?lang=fr.

Au-delà de l'annonce au ton résolument optimiste, il convient de relever que le *Privacy Shield* fait l'objet de très sérieuses critiques[176] et que de nouvelles procédures ont déjà été initiées à son encontre. Ainsi un recours a-t-il déjà été déposé par Digital Rights Ireland pour obtenir l'annulation du feu vert européen au *Privacy Shield*[177].

Quelle qu'en soit l'issue, cet outil de régulation est la démonstration du fait que la protection des données informatiques est une équation dont les variables sont et doivent être constamment réexaminées. Dans un monde de fulgurance et de développements constants, la seule possibilité de pouvoir respecter la loi est d'initier une démarche proactive visant à identifier, respectivement à recenser les fichiers au sein des entreprises et des administrations. Cette première étape nécessite une pleine collaboration des employés qui doivent être orientés sur les buts de cette démarche pour pouvoir y adhérer. Dans une deuxième étape, il faudra évaluer pour chaque fichier si les exigences légales sont satisfaites. Cette étape certes fastidieuse permet d'opérer un tri entre les différents fichiers dont certains ne seront plus à jour. Une telle évaluation de conformité constitue le préalable indispensable à l'analyse des risques. Une fois les risques identifiés et évalués, il sera en définitive possible de prendre les mesures idoines pour les minorer.

Avec l'évolution des normes[178], il n'est plus possible de prendre le risque d'ignorer les obligations légales et de penser que rien ne surviendra, si ce n'est un dommage réputationnel. Le RGPD en est l'illustration parfaite : les entreprises conscientes du champ des possibles sanctions vont tenter de limiter ce risque en recourant à des certifications. Au sein de l'UE, différents acteurs de la protection des données préconisent désormais une collecte très sélective : ne traiter que ce qui est absolument nécessaire. Ce changement de paradigme concerne (certes dans une moindre mesure) la Suisse, même si les sanctions prévues dans l'avant-projet de LPD s'apparentent à un tigre de papier[179], à l'aune de celles figurant dans le RGPD. Les sociétés et même les administrations pourraient à l'aune des activités déployées se trouver un jour, à l'insu de leur plein gré, dans le champ d'application de normes tierces qui, elles, sanctionnent avec la plus grande sévérité les

---

176 A titre exemplatif, http://www.lemonde.fr/pixels/article/2016/07/26/les-gendarmes-europeens-de-la-vie-privee-critiquent-l-accord-privacy-shield_4974925_4408996.html ou encore https://www.cnil.fr/fr/declaration-du-g29-relative-la-decision-de-la-commission-europeenne-concernant-le-privacy-shield et https://techcrunch.com/2016/02/29/lipstick-on-a-pig/.

177 http://www.silicon.fr/privacy-shield-attaque-justice-europeenne-161604.html.

178 Il n'a volontairement pas été fait état de l'avant-projet de loi sur la protection des données dès lors qu'à ce stade, de nombreuses modifications pourraient survenir. Il eût également été possible d'évoquer la modernisation de la Convention 108 sur la protection des données : http://www.coe.int/fr/web/portal/28-january-data-protection-day-factsheet.

179 Cf. notamment l'art. 50 qui fixe le plafond de l'amende à 500'000 francs en cas de violation des obligations de renseigner, de déclarer et de collaborer.

manquements. Rien qu'en raison de la matérialisation possible de ce risque, il convient d'agir très rapidement et d'opérer les contrôles idoines au sein de chaque organisation.

Annexe

Présentation des principales nouveautés engendrées par le règlement européen sur la protection des données pour les entreprises suisses :

Relatives aux principes généraux :

- Obligation de désigner un représentant (art. 27) : les entreprises suisses assujetties au RGPD sans avoir d'établissement en UE doivent désigner un représentant dans l'Union. Exception si le traitement ne concerne pas celui à grande échelle de données sensibles et n'engendre pas de risque pour les personnes concernées.
- Licéité (art. 6) : nécessité de justifier le traitement par un des motifs de l'art. 6 (nécessité à l'exécution d'un contrat, obligation légale, intérêt privé/public, consentement).
- Consentement (art. 7) : niveau élevé pour admettre le consentement de la personne concernée. En plus du caractère libre et éclairé, il doit être spécifique et univoque. Nécessité de séparer le champ réservé au consentement du reste du texte et d'exprimer l'engagement en terme clair et simple. Grand risque de rejet du consentement faute de l'aspect libre si le traitement consenti n'est pas dans le cadre d'exécution du contrat.

  Comme en droit suisse, il est révocable en tout temps, mais l'entreprise a le devoir de l'indiquer. En cas de révocation du consentement, le traitement effectué jusqu'alors est valable. Cependant, la révocation est un motif de l'exercice du droit à l'effacement.
- Devoir d'information active : Les art. 13 et 14 contiennent une longue liste d'informations à fournir spontanément à la personne concernée (y compris pour les données non sensibles).

Relatives aux actions :

- Droit d'accès (art. 15) : davantage d'informations à fournir en cas d'exercice du droit.
- Droit à la portabilité des données (art. 20) : droit de demander les données que la personne a fournies elle-même sur un support lisible par un ordinateur (lorsque les données sont traitées sur la base d'un consentement ou d'un contrat et que le traitement se fait à l'aide de procédés automatisés). Cas échéant, la personne a le droit de les

transmettre à un autre maître du fichier ou de demander que le premier maître du fichier les transmette directement à un autre.

- Droit à l'oubli (art. 17) : motifs permettant à la personne concernée de demander l'effacement des données (donnée plus nécessaire au but, révocation du consentement + pas d'autres justifications au traitement, opposition au traitement ou traitement illicite). Également possibles exceptions permettant au maître du fichier le refus d'effectuer l'effacement.
- Droit à la limitation du traitement (art. 18) : droit de demander à ce que le traitement soit limité à l'enregistrement ou la conservation (sauf en cas d'exceptions). Notamment lorsque l'exactitude de la donnée est contestée (ainsi droit qui va plus loin que la simple mention du caractère litigieux de la donnée de la LPD).
- Droit d'opposition (art. 21) : droit de la personne à s'opposer au traitement lorsque le traitement est justifié par des intérêts publics ou privés (mais possibilité pour l'auteur du traitement de démontrer des intérêts supérieurs). Toutefois droit absolu de s'opposer au traitement si les données sont utilisées à des fins de prospection. Enfin, devoir du maître du fichier d'informer la personne concernée de ce droit de la première prise de contact.
- Décision individuelle automatisée (art. 22) : possibilité pour la personne de demander à ne pas faire l'objet d'une décision fondée uniquement sur un traitement automatisé ou encore de faire l'objet de profiling, si conséquences juridiques pour la personne ou l'affecte de manière similaire. Décision automatisée impossible pour les données sensibles à moins de consentement explicite.

Relatives à l'architecture du système de gestion :

- Privacy by Design (art. 25) : mettre en œuvre en système de traitement qui garantisse la protection des données.
- Privacy by Default (art. 25) : concevoir le système de telle manière à ce que par défaut, seules les données nécessaires à l'accomplissement d'un but spécifique ne soient traitées.
- Data Breach Regulation (art. 33) : en cas de violation de données personnelles, obligation d'informer l'autorité compétente dans un délai allant jusqu'à 72h (en indiquant la nature des données, quantité de données et personnes concernées, conséquences envisagées, mesures prises au moment de la violation) sauf si aucun risque pour les droits et libertés des personnes physiques. Également information des personnes concernées sauf exception (données chiffrées, efforts disproportionnés, risque couvert par les mesures prises).
- Étude d'impact (art. 35) : à faire si le traitement peut présenter un risque particulier. Si le risque est confirmé obligation de consulter l'autorité.

Relatives aux obligations du maître du fichier :

- Maître du fichier doit démontrer la légitimité au RGPD (art. 24).
- Il doit tenir un registre des traitements effectués (à l'exception des petites PME) (art. 30). Le registre contient notamment les finalités, transfert à l'étranger, catégories de personnes concernées, catégories de données, etc.
- Contrat de sous-traitance (art. 28) : grands nombres de conditions et exigences pour la conclusion d'un contrat de sous-traitance.
- Obligation de nommer un délégué à la protection des données (art. 37) en cas de suivi régulier et systématique à grande échelle ou traitement à grande échelle de données sensibles.

Relatives aux sanctions :

- Actions correctrices (art. 58) : l'autorité dispose d'un très large spectre de mesures correctrices qu'elle peut imposer à l'entreprise.
- Amendes administratives (art. 83) : selon les caractéristiques de chaque cas, l'autorité compétente a la possibilité en plus ou à la place des mesures correctrices de fixer des amendes administratives. Dans les cas les plus graves, les amendes les plus élevées peuvent s'élever à 20 millions d'euros ou, dans le cas d'une entreprise, 4% de chiffre d'affaires mondial total du précédent exercice.
- Sanctions de l'État membre (art. 84) : le droit national d'un État membre peut fixer d'autres sanctions notamment pour les violations qui ne font pas l'objet d'amendes administratives.
- À réserver encore les possibilités d'actions en réparation du dommage ou du tort moral exercé par les personnes concernées (art. 82).

Bibliographie

ALO EDWARD, EU Privacy Protection : a Step Towards Global Privacy, *in* : Michigan State International Law Review, 22 (3) 2014, pp. 1100 ss, disponible en ligne sur : http://digitalcommons.law.msu.edu/ilr/vol22/iss3/11/.

ANCELLE JULIETTE, Droit de l'Internet et des nouvelles technologies : le droit rattrapera-t-il Internet ? *in* : Regards de marathoniens sur le droit suisse, Mélanges publiés à l'occasion du 20e « Marathon du droit », Genève 2015, pp. 195 ss.

ANCELLE JULIETTE/JACCARD MICHEL, Protection des données, kit du praticien, *in* : Revue de l'avocat 9/2014, pp. 369 ss.

BAERISWYL BRUNO, Commentaire de l'art. 6 LPD, *in* : Bruno Baeriswyl/Kurt Pärli (éds.), Datenschutzgesetz (DSG) – Handkommentar, Berne 2015.

BONNET FLORENCE, Les labels de protection des données personnelles sont source de valeur ajoutée, *in* : Revue Banque n° 769, 29 janvier 2014, disponible en ligne sur : http://www.revue-banque.fr/risques-reglementations/article/les-labels-protection-des-donnees-personnelles-son.

CHABOT FLAVIO-GABRIEL, La protection des données à la lumière de deux exemples tirés de l'actualité récente, *in* : Bulletin Cedidac n° 57, octobre 2011, disponible en ligne sur : http://www.unil.ch/files/live//sites/cedidac/files/Bulletins/Bulletin_no_57.pdf.

COTTIER BERTIL, Gouvernance d'Internet : protection de la vie privée et des données personnelles, *in* : Swiss Review of International and European Law, 26 (2) 2016, pp. 255-272.

COTTIER BERTIL, Quoi de Neuf à l'Etranger, Essai de bilan de l'activité récente des législateurs européens et américains, *in* : Astrid Epiney/Tobias Fasnacht/Gaëtan Blaser, Instruments de mise en œuvre du droit à l'autodétermination informationnelle, Zurich/Genève 2013, pp. 67-85 (cité : COTTIER, Quoi de Neuf).

COTON FANNY/HENROTTE JEAN-FRANÇOIS, Application territoriale de la législation européenne en matière de protection des données et transfert de données vers des pays tiers : vaincre la peur de l'autre, *in* : Les enjeux européens et mondiaux de la protection des données personnelles, Bruxelles, 2015, pp. 171-217.

DUNAND JEAN-PHILIPPE, Internet au travail : droits et obligations de l'employeur et du travailleur, *in* : Jean-Philippe Dunand/Pascal Mahon (éds.), Internet au travail, Genève/Zurich/Bâle 2014, pp. 33-71.

FANTI SÉBASTIEN, Bref aperçu des aspects légaux du BYOD (Bring Your Own Device), *in* : Jean-Philippe Dunand/Pascal Mahon (éds.), Internet au travail, Genève/Zurich/Bâle 2014, pp. 165 ss.

FANTI SÉBASTIEN, La notion de document officiel en droit fédéral et en droit valaisan, *in* : RVJ 2016, pp. 393-440 (cité : FANTI, La notion de document officiel).

FLUECKIGER ALEXANDRE/DAHMEN STEPHANIE, Jurisprudence actuelle en matière de protection des données, *in* : Big Data et droit de la protection des données, Zurich 2016, pp. 127-141.

FUHRER STEPHAN, Pensionskassenausweise, *in* : HAVE 3/2012, pp. 298-300.

HACK MICHAEL, L'intelligence artificielle a des superpouvoirs de cybersécurité… 60 ans après sa création, *in* : L'Usine digitale, 18 avril 2016, disponible en ligne sur : http://www.usine-digitale.fr/article/l-intelligence-artificielle-a-des-super-pouvoirs-de-cybersecurite-60-ans-apres-sa-creation.N387416.

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

MÉTILLE SYLVAIN, Jurisprudence actuelle en matière de protection des données : Surveillance, infiltration et transmission de données à un tiers : quelques atteintes à la sphère privée qui ont occupé récemment les tribunaux, *in* : Astrid Epiney/Tobias Fasnacht/Gaëtan Blaser, Instruments de mise en œuvre du droit à l'autodétermination informationnelle, Zurich/Genève 2013, pp. 113-124.

MÉTILLE SYLVAIN, La surveillance électronique des employés, *in* : Jean-Philippe Dunand/Pascal Mahon (éds.), Internet au travail, Genève/Zurich/Bâle 2014, pp. 99-132 (cité : MÉTILLE, La surveillance électronique).

MIGNOT HERVÉ, Tribune : doit-on voter une loi du drapeau rouge pour l'Intelligence Artificielle ?, *in* : Numerama, 5 janvier 2017, disponible en ligne sur : http://www.numerama.com/

politique/222569-tribune-doit-on-voter-une-loi-du-drapeau-rouge-pour-lintelligence-artificielle.html.

MORIN JEAN-HENRY, L'utilisation des moyens techniques en vue d'une amélioration de la protection des données, *in* : Astrid Epiney/Tobias Fasnacht, Le développement du droit européen en matière de protection des données et ses implications pour la Suisse, Zurich 2012, pp. 1-12.

WALTER JEAN-PHILIPPE, L'effectivité des mécanismes de mise en œuvre de la protection des données : Le point de vue du Préposé fédéral à la protection des données et à la transparence (PFPDT), en bref, *in* : Astrid Epiney/Daniela Nüesch (éds.), La mise en œuvre des droits des particuliers dans le domaine de la protection des données, Zurich 2015, pp. 115-124.

WINKLER MARIA, La protection des données dans l'entreprise – Un mode d'emploi pour sa mise en œuvre, *in* : TREX L'expert fiduciaire 2/2011, pp. 109-113.