CERT

Anne-Sylvie Dupont | Pascal Mahon (éds)

François Chanson I Jean-Philippe Dunand I
Anne-Sylvie Dupont I Karine Lempen I
Marco Meli I Sylvain Métille

La fin des rapports de travail

unine
UNIVERSITÉ DE NEUCHÂTEL
FACULTÉ DE DROIT

Schulthess
ÉDITIONS ROMANDES

Anne-Sylvie Dupont | Pascal Mahon (éds)

François Chanson I Jean-Philippe Dunand I
Anne-Sylvie Dupont I Karine Lempen I
Marco Meli I Sylvain Métille

La fin des rapports de travail

CERT
Centre d'étude
des relations de travail

Schulthess
ÉDITIONS ROMANDES
§ 2021

Citation suggérée de l'ouvrage : Anne-Sylvie Dupont | Pascal Mahon (éds), *La fin des rapports de travail,* « Collection CERT », Genève / Zurich 2021, Schulthess Éditions Romandes

ISBN 978-3-7255-8779-7

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 SPRL, Avenue Milcamps 119, B-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

SYLVAIN MÉTILLE*

Après la fin des rapports de travail, peut-on encore traiter des données personnelles ?

Sommaire

* Je remercie sincèrement M. Livio di Tria pour sa précieuse aide dans la rédaction de cette contribution, ainsi que Mme Annelise Ackermann et Me David Raedler et pour leurs conseils avisés.

I. Introduction

La présente contribution n'a pas l'ambition d'analyser sous toutes ses coutures le droit de la protection des données dans les rapports de travail de droit privé. Nous nous contentons de présenter d'abord le cadre juridique (II) et les principes fondamentaux de la protection des données (III), ainsi que le traitement et la conservation des données, avant, pendant et après les rapports de travail (IV et V). Nous passerons ensuite en revue quelques obligations et possibilités de conserver des données personnelles après la fin des rapports de travail (VI), pour terminer avec quelques remarques pratiques (VIII).

II. Le cadre juridique

A. La Loi fédérale sur la protection des données

Tout traitement de données personnelles par des personnes privées ou par des organes fédéraux est régi par la Loi fédérale sur la protection des données (LPD)[1]. Le traitement par des autorités cantonales au sens large (y compris d'éventuelles personnes privées délégataires de tâches publiques cantonales) est quant à lui régi par les lois cantonales de protection des données qui contiennent des dispositions similaires à celles du régime de la LPD applicable aux organes fédéraux[2].

On ne le répétera jamais assez, le but de la protection des données n'est pas de protéger une donnée en tant que telle[3], mais de protéger la personnalité des personnes dont les données sont traitées. Il ne s'agit donc pas d'interdire tout traitement de données personnelles, mais bien plus de l'encadrer pour qu'il se déroule de manière conforme aux principes généraux institués par le législateur[4]. En ce sens, la LPD concrétise, pour les traitements effectués par des personnes privées, la protection de la personnalité protégée

1 LPD ; RS 235.1.

2 MEIER, N 356 ; BSK DSG-MAURER-LAMBROU/KUNZ, N 13 ss *ad* art. 2 ; ROSENTHAL/JÖHRI, N 4 ss *ad* art. 2 ; BELSER, *in* : Belser/Epiney/Waldmann, N 4 ss *ad* § 5.

3 Ce serait juridiquement plutôt dans les domaines du droit d'auteur ou de la concurrence déloyale qu'une protection des données en tant que telles pourraient se trouver. A noter que la protection de la donnée en tant que telle est toutefois prévue par le principe de sécurité qui exige que le responsable du traitement et le sous-traitant prennent les mesures techniques et organisationnelles nécessaires pour éviter toute perte, modification ou accès indu à des données personnelles.

4 Evidemment dans certaines situations un traitement de données ne pourra pas avoir lieu de manière licite et sera purement et simplement interdit.

par l'art. 28 du Code civil suisse[5] et, en matière de traitements effectués par des organes fédéraux, la protection du droit à l'autodétermination informationnelle telle qu'ancrée à l'art. 13 al. 2 de la Constitution fédérale de la Confédération suisse[6].

La LPD a fait l'objet d'un long processus de révision totale[7] qui a abouti à l'adoption par l'Assemblée fédérale le 25 septembre 2020 du texte final de la LPD révisée (nLPD)[8]. La structure et les principes généraux demeurent, mais de nouveaux droits et obligations ont été introduits, ainsi que de nouvelles formalités.

En bref, on peut mentionner l'ajout des principes de protection des données dès la conception et par défaut[9], ainsi qu'un renforcement du principe de transparence avec une obligation générale d'informer[10]. Cette obligation n'existait précédemment que pour le traitement de données sensibles et de profils de la personnalité[11] ou le traitement de données par l'administration[12], la simple reconnaissabilité étant suffisante dans les autres cas[13]. Les nouvelles formalités sont principalement la tenue du registre des activités de

5 CC ; RS 210.

6 Cst. ; RS 101.

7 Révisée partiellement plusieurs fois depuis son entrée en vigueur le 1er juillet 1993, la révision totale a officiellement débuté le 1er avril 2015 lorsque le Conseil fédéral a chargé le Département fédéral de justice et police d'examiner les mesures législatives à prendre pour renforcer la protection des données, notamment au vu des évolutions technologiques toujours plus rapides. Les premières réflexions étaient bien antérieures puisqu'elles avaient déjà commencé en 2010, lorsque l'Office fédéral de la justice s'est lancé dans une évaluation de la LPD, ayant abouti à l'adoption par le Conseil fédéral du rapport sur l'évaluation de la Loi fédérale sur la protection des données (FF 2012 255-272). Le Conseil fédéral a publié son message (FF 2017 6565-6802) accompagné du projet de nouvelle loi (FF 2017 6803-6884) le 15 septembre 2017. Les discussions ont été longues et compliquées entre les Chambres fédérales et ce n'est qu'après avoir épuisé tous les aller-retours possibles qu'une séance de conciliation a été tenue pour permettre l'adoption d'un texte en vote final par les deux chambres. Pour les détails de la procédure de révision, voir : www.parlament.ch/fr/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20170059 (consulté le 4 janvier 2021). Voir également sur la nLPD ROSENTHAL.

8 BO 2020 N 1994 ; BO 2020 E 1081.

9 Art. 7 al. 1 et 2 nLPD en ce qui concerne la protection des données dès la conception et art. 7 al. 3 nLPD pour la protection des données par défaut. Ces deux principes sont également ancrés à l'article 25 du Règlement européen sur la protection des données (RGPD) et le Comité européen de la protection des données a publié ses lignes directrices 4/2019 précisant ces principes. Voir également TAMÒ-LARRIEUX.

10 Art. 19 et 20 nLPD.

11 Art. 14 LPD.

12 Art. 18a et 18b LPD.

13 Art. 4 al. 4 LPD.

traitements[14] qui remplace la déclaration des fichiers[15], l'analyse d'impact relative à la protection des données et la consultation préalable du Préposé fédéral à la protection des données et à la transparence (PFPDT) dans ce cadre[16], l'obligation d'information en cas de violation de la sécurité des données[17] et en cas de décision automatisée[18]. La personne concernée peut aussi faire valoir un droit à la remise ou à la transmission des données personnelles (droit à la remise ou portabilité)[19]. Les pouvoirs du PFPDT sont (modestement) renforcés[20], des amendes pénales sont prévues dans des situations un peu plus larges qu'actuellement (mais demeurent limitées)[21] et la gratuité de la procédure judiciaire est introduite[22]. Finalement, la terminologie est en grande partie unifiée avec le droit cantonal et européen. On ne parle plus de maître du fichier, mais de responsable du traitement, sans que cela n'apporte de changement matériel[23].

Nous ferons donc référence tant au droit actuellement en vigueur (LPD), qu'au droit futur (nLPD) étant donné que l'entrée en vigueur de la nLPD est attendue pour 2022.

Pour le lecteur qui est peu familier du domaine, il est utile de rappeler quelques notions propres à la protection des données.

Premièrement, la notion de données personnelles est large et couvre toutes les données liées à une personne identifiée ou identifiable[24]. La LPD protège tant les données des personnes physiques que des personnes morales[25], alors que la nLPD ne protège plus les

14 Art. 12 nLPD. Le registre des activités de traitement doit notamment contenir dans la mesure du possible, le délai de conservation des données personnelles ou, à défaut, les critères pour déterminer la durée de conservation.

15 Art. 11a LPD.

16 Art. 22 et 23 nLPD.

17 Art. 24 nLPD.

18 Art. 21 nLPD.

19 Art. 28 et 29 nLPD.

20 Art. 49 ss nLPD. Notamment l'art. 51 nLPD qui permet dorénavant au PFPDT de prononcer des mesures administratives plutôt que de « simples » recommandations.

21 Art. 60 ss nLPD.

22 La révision totale de la Loi fédérale sur la protection des données introduira deux nouveaux articles, prévoyant la gratuité de la procédure, au sein du Code de procédure civile du 19 décembre 2008 (CPC ; RS 272). Il s'agit des nouveaux art. 113 al. 2 let. g (procédure de conciliation) et 114 let. g (procédure au fond).

23 La LPD du 19 juin 1992, ainsi que certains droits cantonaux, utilisent le terme de « maître du fichier ». Pour des raisons d'uniformisation en vue de l'entrée en vigueur de la nLPD, telle qu'adoptée par le Parlement fédéral le 25 septembre 2020, nous recourrons déjà à la nouvelle appellation.

24 MEIER, N 424 ss ; BSK DSG-BLECHTA, N 3 ss *ad* art. 3 ; ROSENTHAL/JÖHRI, N 1 ss *ad* art. 3 ; MÉTILLE, Internet et droit, pp. 79-80.

25 Art. 2 al. 1 LPD.

données des personnes morales[26]. Elle rejoint ainsi la plupart des législations étrangères en matière de protection des données, y compris le RGPD.

Une personne est identifiée lorsque l'on sait de qui il s'agit[27], par exemple le travailleur Dupond. Elle est identifiable lorsqu'elle n'est pas encore identifiée, mais peut l'être directement ou indirectement, sur la base de l'information concernée et d'un ou plusieurs autres éléments. Tel sera par exemple le cas de l'utilisateur de l'ordinateur numéro IUD438[28]. Un nom, une adresse électronique, un numéro de téléphone, une adresse IP[29], un numéro AVS, une empreinte digitale, une adresse ou une date de naissance peuvent ainsi constituer des données personnelles d'une personne identifiable. La seule date de naissance, sans autre indication, ne constitue pas en soi une donnée personnelle. Elle le devient lorsqu'elle est, par exemple, corrélée à un nom et que le responsable du traitement est en mesure d'identifier la personne sur la base de cette combinaison d'éléments[30]. La possibilité d'identification peut toutefois intervenir sur la base d'un seul élément comme une adresse électronique[31] ou un numéro d'identification unique tel que le numéro AVS[32].

Les données pseudonymes[33] sont typiquement des données personnelles relatives à une personne identifiable. Si une identification n'est pas possible, on parle alors de données anonymes qui, elles, sortent du champ d'application de la protection des données. La qualification juridique des données pseudonymisées a fait l'objet, au sein de la doctrine, de nombreuses controverses[34]. Ces dernières portent essentiellement sur la question de savoir de quel point de vue il convient d'apprécier la possibilité d'identifier une personne. Ainsi, on oppose l'approche dite « alternative » à l'approche dite « relative ». Dans la première approche, les données pseudonymisées constituent en tous les cas des données personnelles, car l'exportateur des données est à même d'identifier les personnes

---

26 Art. 2 al. 1 nLPD. La protection générale des art. 28 ss du Code civil suisse du 10 décembre 1970 (CC ; RS 210) continue de s'appliquer aux personnes physiques et morales.

27 MEIER, N 431 ; BSK DSG-BLECHTA, N 7 *ad* art. 3 ; ROSENTHAL/JÖHRI, N 6 *ad* art. 3.

28 MEIER, N 432 ; BSK DSG-BLECHTA, N 10 *ad* art. 3 ; ROSENTHAL/JÖHRI, N 18 ss *ad* art. 3.

29 MEIER N 446 et 447 ; MEIER/TSCHUMY, pp. 5-6 ; ATF 136 II 508, c. 3.5 ; Arrêt CJUE *Patrick Breyer c/Bundesrepublik Deutschland*, C-582/14 du 19 octobre 2016, § 49.

30 MEIER, N 433.

31 sylvain.metille@unil.ch.

32 MEIER, N 433.

33 Le RGPD définit la pseudonymisation comme le traitement de données personnelles de telle façon que celles-ci ne puissent plus être attribuées à une personne concernée précise sans avoir recours à des informations supplémentaires, pour autant que ces informations supplémentaires soient conservées séparément et soumises à des mesures techniques et organisationnelles afin de garantir que les données personnelles ne sont pas attribuées à une personne physique identifiée ou identifiable.

34 MEIER, N 437 ss ; BSK DSG-BLECHTA, N 12-13 *ad* art. 3 ; ROSENTHAL/JÖHRI, N 37 ss *ad* art. 3.

concernées grâce à la table de concordance. La seconde approche, désormais confirmée par le Tribunal fédéral, retient que la possibilité d'identifier la personne concernée doit s'apprécier de façon relative, soit selon le point de vue de l'intéressé[35]. Ainsi, des données pseudonymisées constituent des données personnelles du point de vue de celui qui détient la table de concordance, mais également de celui qui peut réidentifier la personne concernée en mettant en œuvre des moyens raisonnables[36]. Ne sont pas raisonnables des moyens interdits par la loi ou irréalisables en pratique (ou au prix d'efforts démesurés en termes de temps, de coût et de main d'œuvre). Ces données seront donc des données anonymes pour celui pour qui l'identification n'est pas envisageable par des moyens raisonnables.

Deuxièmement, il faut s'intéresser aux acteurs en présence et leurs rôles. On distingue traditionnellement la personne concernée[37], le responsable du traitement[38], et cas échéant le sous-traitant[39]. Tous les autres sont des tiers[40].

La personne concernée est celle dont les données personnelles sont traitées[41]. Quant au responsable du traitement, c'est celui qui détermine les finalités et les moyens du traitement de données personnelles. Dans le cadre de la relation de travail, le travailleur sera généralement la personne concernée et l'employeur le responsable du traitement[42]. Le responsable du traitement peut aussi se faire aider par un sous-traitant, soit une personne qui traite des données personnelles pour le compte et selon les instructions du responsable du traitement[43]. On parle parfois encore de destinataire : ce n'est rien d'autre que celui qui

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

36 TF 4A_365/2017 du 26 février 2018, c. 5.1.2 ; voir également Arrêt CJUE *Patrick Breyer c/Bundesrepublik Deutschland*, C-582/14 du 19 octobre 2016, § 42-46 ; FF 2017 6639-6640.

37 Art. 3 let. b LPD ; art. 5 let. b nLPD.

38 Art. 3 let. i LPD ; art. 5 let. j nLPD.

39 La LPD ne définit pas le « sous-traitant », toutefois l'art. 10a LPD prévoit certaines règles légales à respecter en cas de « traitement de données par un tiers ». S'agissant de la nLPD, une définition a été introduite à l'art. 5 let. k nLPD alors que l'art. 9 nLPD reprend en partie les règles légales ancrées à l'art. 10a LPD.

40 Le Comité européen de la protection des données a publié les Guidelines 07/2020 sur les notions de responsable du traitement et de sous-traitant. Ces lignes directrices reviennent sur les notions précitées et sont agrémentées d'exemples pratiques aidant à différencier chaque rôle.

41 PFPDT, Guide 2014, p. 3.

42 MEIER, N 2031. Si l'employeur est une personne morale, le travailleur pourrait traiter les données en tant que responsable du traitement (au nom de l'employeur) et être la personne concernée. Par exemple, la personne en charge des salaires traite les données personnelles des travailleurs (y compris les siennes) au nom de l'employeur.

43 Art. 10a LPD ; 9 nLPD.

reçoit des données. Juridiquement, il peut s'agit d'un responsable du traitement (indépendant) ou d'un sous-traitant[44].

B. Le droit du travail

Le droit du travail se compose d'une multitude de règles intégrant essentiellement le Code des obligations[45], la Loi sur le travail[46] et ses ordonnances, ainsi que les éventuelles Conventions collectives de travail (CCT) ou contrats-types de travail (CTT).

Sous l'angle particulier du traitement des données personnelles, l'art. 328b CO a été inséré en 1993 par la LPD pour protéger la personnalité du travailleur et reprend la règle générale de l'art. 28 CC[47]. Cet ajout s'explique en raison du fait que, au sein d'un rapport juridique aussi fort que celui d'une relation de travail, les opérations de traitement et les types de données personnelles sont nombreux. De plus, les données personnelles peuvent être conservées pendant une longue durée[48]. S'y ajoute aussi le fait que le rapport de subordination existant entre le travailleur et l'employeur pourrait également mener le second à imposer un grand nombre de traitements au premier, sans que celui-ci n'ait la possibilité de s'y opposer. Enfin, et sans égard aux opérations de traitement ou aux types de données personnelles, l'introduction d'une telle disposition légale s'explique aussi en raison des nombreux rapports contractuels de travail.

Selon l'art. 328b CO, 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. Il précise encore que les dispositions de la LPD sont applicables. La question de la portée de cette disposition a été très controversée en doctrine, notamment sur le sens à donner au renvoi à la LPD[49].

Pour une partie de la doctrine, l'art. 328b CO ne dispose pas d'une réelle portée pratique et ne fait que reprendre les principes prévus par la LPD, notamment le principe de proportionnalité et celui de finalité. Pour une autre partie, l'art. 328b CO dérogerait aux règles générales de la protection des données en limitant, légalement, les finalités pour lesquelles un employeur est autorisé à collecter et traiter des données personnelles. Un tel courant de doctrine exclurait *per se* d'autres finalités et interdirait tout recours aux motifs

---

44 FF 2017 6770.

45 CO ; RS 220.

46 LTr ; RS 822.11.

47 WYLER, p. 433 ; MEIER, N 2018.

48 MEIER, N 2020.

49 MEIER, N 2033-2035 ; DUNAND, *in :* Dunand/Mahon, N 6 *ad* art. 328b ; MEIER, N 2032-2035 ; RAEDLER, p. 150 ; WYLER, p. 433 ; CARRUZZO, p. 319 ; CR CO I-AUBERT, N 2 *ad* art. 328b.

justificatifs prévus par la LPD. Finalement, pour une troisième partie, l'art. 328b CO constitue une *lex specialis* à l'art. 13 LPD[50].

Dans un arrêt récent, le Tribunal fédéral a appliqué les motifs justificatifs de l'art. 13 LPD dans le cadre d'une relation de travail[51]. Il a donc confirmé que l'art. 13 LPD peut être appliqué également dans le cadre de l'art. 328b CO, refusant ainsi l'exclusion de cette disposition – et du mécanisme de la LPD – dans les rapports de travail. Malheureusement, le Tribunal fédéral ne s'est pour le reste pas prononcé sur la portée de l'art. 328b CO et la controverse doctrinale.

Il est en revanche admis que l'art. 328b CO s'applique également après la fin des rapports de travail, pour autant que les traitements de données découlent des rapports de travail[52].

A toutes fins utiles, il faut encore mentionner l'Ordonnance 3 du 18 août 1993 relative à la Loi sur le travail (OLT 3)[53], en particulier son art. 26. Ce dernier prévoit le principe selon lequel un employeur ne peut avoir recours à des systèmes de surveillance ou de contrôle destiné à surveiller le comportement des travailleurs à leur poste de travail. Il peut cependant y avoir recours pour « d'autres raisons ». Dans ce cas, les systèmes doivent être conçus et disposés de façon à ne pas porter atteinte à la santé et à la liberté de mouvement des travailleurs. Cette disposition légale joue un rôle certain dans le cadre de l'exécution d'un contrat de travail mais nous ne procéderons pas un examen approfondi de toutes ses composantes, celle-ci ne concernant pas la fin des rapports de travail ; qui plus est, pareil examen a déjà été fait[54].

III. Les principes fondamentaux de protection des données

La LPD, comme la nLPD, ancre en son sein une présomption irréfragable d'atteinte à la personnalité lorsque des données personnelles sont traitées en violation des principes qui seront passés en revue ci-dessous[55]. Cette atteinte à la personnalité peut néanmoins être guérie et considérée comme licite si elle peut être justifiée par le consentement de la

50 MEIER, N 2033-2035 et références citées, RAEDLER, p. 150 et les références citées.
51 TF 4A_588/2018 du 17 juin 2019, c. 4.3.
52 MEIER, N 2071, CARRUZZO, p. 319 ; et DUNAND, N 5.
53 OLT 3 ; RS 822.113.
54 MÉTILLE SYLVAIN, Surveillance et les références citées.
55 Art. 12 al. 2 let. a LPD et art. 30 al. 2 let. a nLPD.

personne concernée, un intérêt prépondérant privé, un intérêt prépondérant public, ou par la loi[56].

Les principes fondamentaux en matière de protection des données sont le principe de licéité[57], de bonne foi[58], de proportionnalité[59], de finalité[60], de transparence[61], d'exactitude[62] et de sécurité[63]. Depuis l'adoption de la nouvelle LPD, le principe de protection des données dès la conception[64] et le principe de protection des données par défaut[65] s'ajoutent à ce catalogue.

La jurisprudence récente a eu l'occasion de préciser, si besoin était, que le principe de licéité doit se comprendre comme l'absence de violation d'une norme impérative du droit de la protection des données ou d'une norme visant à protéger la personnalité hors LPD[66]. Autrement dit, un traitement de données personnelles viole le principe de licéité s'il contrevient à une norme de droit impératif destinée à protéger la personnalité.

Le principe de bonne foi est un principe général de l'ordre juridique suisse (art. 2 CC). Dans le domaine de la protection des données, celui-ci se traduit notamment par le fait qu'aucune donnée ne doit être traitée à l'insu de la personne concernée ou contre sa volonté[67]. Il est également exclu pour le responsable du traitement de mentir à la personne concernée sur les traitements allant être faits ou les buts poursuivis.

Le principe de proportionnalité, qui sous-tend plus largement l'ordre juridique suisse à bien des égards, se divise classiquement en trois règles[68] : celle de la nécessité, de l'aptitude ou de l'adéquation, ainsi que celle de la proportionnalité au sens étroit. Ainsi l'employeur ne peut traiter que les données personnelles qui sont objectivement nécessaires et aptes à atteindre le but poursuivi, et pour autant que le traitement demeure

---

56 Art. 13 LPD et art. 31 nLPD. A noter que le RGPD prévoit un système différent avec l'exigence systématique d'un motif justifiant le traitement (art. 6 ou 9 RGPD).

57 Art. 4 al. 1 LPD ; art. 6 al. 1 nLPD.

58 Art. 4 al. 2 LPD ; art. 6 al. 2 nLPD.

59 Art. 4 al. 2 LPD ; art. 6 al. 2 nLPD.

60 Art. 4 al. 3 LPD ; art. 6 al. 3 nLPD.

61 Art. 4 al. 4 LPD et les obligations d'information des art. 14 et 18a LPD, ainsi que 19 nLPD.

62 Art. 5 LPD ; art. 6 al. 5 nLPD.

63 Art. 7 LPD ; art. 8 nLPD.

64 Art. 7 al. 1 et 2 nLPD.

65 Art. 7 al. 3 nLPD.

66 TAF A-3548/2018 du 19 mars 2019.

67 MEIER, N 649 ; MÉTILLE, Internet et droit, p. 83 ; BSK DSG-MAURER-LAMBROU/STEINER, N 7 ss *ad* art. 4 ; ROSENTHAL/JÖHRI, N 14 ss *ad* art. 4.

68 MEIER, N 665 ; MÉTILLE, Internet et droit, pp. 83-84 ; BSK DSG-MAURER-LAMBROU/STEINER, N 9 ss *ad* art. 4 ; ROSENTHAL/JÖHRI, N 14 ss *ad* art. 4 ; WALDMANN/OESCHGER, *in* : Belser/Epiney/Waldmann, N 64 ss *ad* § 13.

dans un rapport raisonnable entre le résultat légitime recherché et le moyen utilisé, tout en préservant le plus possible les droits du travailleur[69]. C'est aussi du principe de proportionnalité que découlent les sous-principes de minimisation des données[70] et de limitation de la durée de conservation des données[71]. Le principe de la proportionnalité s'applique au mode de traitement, à l'étendue des données récoltées, traitées et conservées, à la nature des données ainsi qu'à l'accès aux données ou à leur communication à des tiers[72].

Le principe de finalité, aussi appelé parfois principe de respect du but, implique que des données personnelles ne peuvent être traitées que pour des finalités déterminées. Une collecte de données pour des buts encore inconnus ou vagues n'est pas permise. Cela s'apprécie évidemment selon les circonstances, l'objectif étant principalement de concilier les intérêts des personnes concernées et ceux du responsable du traitement[73]. La nLPD précise désormais que les données peuvent également être traitées ultérieurement de manière compatible avec les finalités initiales[74]. Cette nouvelle formulation n'implique toutefois pas de changement majeur. On considère déjà aujourd'hui que si la personne concernée transmet son adresse, par exemple dans le cadre d'une commande, l'utilisation ultérieure de cette adresse à des fins commerciales peut être considérée comme compatible avec le principe de finalité[75]. Un traitement ultérieur ne sera toutefois pas admissible si la personne concernée peut légitimement le considérer comme inattendu, inapproprié ou contestable[76].

Le principe de transparence prévoit que le traitement de données personnelles ne doit pas avoir lieu à l'insu de la personne concernée. Au contraire, la personne doit être informée. Si la LPD se contente encore dans une large mesure d'une simple reconnaissabilité[77], ce n'est pas le cas de la nLPD et du RGPD[78] qui exigent un véritable devoir d'information. En effet, selon l'art. 19 nLPD, le responsable du traitement (privé et public)[79] doit informer la personne concernée de manière adéquate de la collecte de données personnelles et lui

69 MEIER, N 666.
70 MEIER, N 673 ; MÉTILLE, pp. 83-84.
71 MEIER, N 679 ss.
72 MEIER, N 676.
73 MEIER, N 723.
74 Art. 6 al. 3 nLPD.
75 FF 2017 6645 ; MEIER, N 731.
76 FF 2017 6645.
77 Le devoir d'informer ne s'applique que lors du traitement de données sensibles et de profils de la personnalité par un responsable du traitement privé (art. 14 LPD) et dans tous les cas de traitement par un organe fédéral (art. 18a LPD).
78 Art. 12 à 14 RGPD.
79 Seules les exceptions diffèrent (art. 20 nLPD). Voir ROSENTHAL, N 92 ss.

communiquer au moins certaines informations, telles que l'identité et les coordonnées du responsable du traitement. Il est néanmoins précisé que la liste des informations à fournir est moins détaillée dans la nLPD que dans le RGPD.

Le principe d'exactitude exige de celui qui traite des données personnelles qu'il s'assure qu'elles sont correctes, actuelles et objectives. L'obligation d'exactitude n'est pas absolue, mais elle doit être proportionnée à la finalité du traitement[80]. Il faut donc prendre toutes les mesures appropriées qui permettent de rectifier, d'effacer ou de détruire les données personnelles inexactes ou incomplètes au regard des finalités pour lesquelles elles sont collectées ou traitées[81]. Ce principe consacre aussi un droit de la personne concernée à faire corriger une donnée personnelle inexacte[82].

Le principe de sécurité exige que des mesures techniques et organisationnelles appropriées garantissent une sécurité adéquate des données personnelles par rapport au risque encouru. Il faut notamment éviter toute perte de données personnelles, leur modification, leur effacement ou leur destruction, leur divulgation ou un accès non autorisé à ces données, et ce indépendamment de la question de savoir si la violation est intentionnelle ou non, licite ou illicite[83]. Ces mesures peuvent viser par exemple à pseudonymiser des données, à chiffrer les supports ou à contrôler les accès. S'y ajoute également la mise en œuvre de processus permettant d'identifier l'existence d'une faille de sécurité et de respecter les obligations d'annonce qui s'appliquent.

Le nouveau principe de protection des données dès la conception impose au responsable du traitement de mettre en place, dès la conception du traitement, des mesures techniques et organisationnelles afin de garantir le respect des prescriptions en matière de protection des données[84], alors que la protection des données par défaut doit garantir, par le biais de préréglages appropriés, que le traitement de données est limité au minimum requis par la finalité poursuivie, à moins que la personne concernée n'en dispose autrement[85]. Déjà ancré au sein de la législation européenne en matière de protection des données, ces notions sont détaillées par les lignes directrices 4/2019 du Comité européen de la protection des données[86], ces dernières pouvant servir de source d'inspiration.

---

80 MEIER, N 745 et 752 ; BSK DSG-MAURER-LAMBROU/SCHÖNBÄCHLER, N 5 *ad* art. 5 ; MÉTILLE, Internet et droit, p. 86.

81 TAF 4A_4232/2015 du 18 avril 2017.

82 Art. 5 al. 1 et 15 al. 2 LPD ; art. 6 al. 5 et 32 al. 3 nLPD.

83 MEIER, N 780 ss ; BSK DSG-STAMM-PFISTER, N 15 ss.

84 Art. 7 al. 1 et 2 nLPD. Voir notamment ROSENTHAL, N 43-47.

85 Art. 7 al. 3 nLPD. Voir notamment ROSENTHAL N 47-52.

86 Guidelines 4/2019 on Article 25 Data Protection by Design and by Default du 13 novembre 2019, accessibles uniquement en langue anglaise pour le moment.

IV. Le traitement et la conservation de données avant et pendant les rapports de travail

L'employeur peut donc traiter des données personnelles concernant le travailleur dans le respect des principes précités, et cela avant, pendant et après la relation de travail. Les principes de licéité, de bonne foi, de transparence, d'exactitude, de sécurité, de protection des données dès la conception et de protection des données par défaut ne devraient pas soulever de problèmes juridiques particuliers. Ils impliqueront toutefois des mesures pratiques pour s'assurer de leur respect.

Il en va différemment pour les principes de proportionnalité et de finalité. Le premier parce que l'intérêt à traiter certaines données diminue avec l'écoulement du temps et le second parce que les buts du traitement ne sont pas les mêmes qu'il existe encore ou non une relation de travail.

Avant le début de la relation de travail, l'employeur va traiter des données personnelles portant sur les aptitudes du candidat à remplir le poste visé. Il ne pourra demander au candidat que les informations dont il a besoin pour déterminer s'il satisfait aux exigences du poste[87].

Un dossier de candidature peut contenir des documents variés comme une lettre de motivation, un *curriculum vitae*, des diplômes, des certificats de travail, des lettres de recommandation, etc. Tous ces documents contiennent de nombreuses données personnelles[88].

L'employeur ne pouvant traiter que les informations nécessaires et aptes à vérifier l'aptitude du candidat, les données pouvant légitimement être traitées dépendront du poste concerné. Interroger un candidat sur des maladies existantes, le souhait d'avoir des enfants ou un endettement éventuel ne pourra être admis que si des raisons particulières l'exigent[89]. Le contrôle d'antécédents ou le contrôle de sécurité (*background check*) n'est admis que de manière restrictive et avec le consentement du candidat[90].

---

87 PFPDT, Guide 2014, p. 8.

88 Nom, prénom, date de naissance, nationalité, adresse électronique, numéro de téléphone, domicile, état civil, photo, résultats scolaires, style d'écriture, etc.

89 PFPDT, Guide 2014, p. 8. Les questions liées à un éventuel endettement seront par exemple admises si le candidat postule comme convoyeur de fonds ou comme agent de sécurité devant faire des rondes au sein d'une institution bancaire. De même, les questions liées à la santé du candidat seront admises pour autant que le poste nécessite, par exemple, la manipulation de produits dangereux.

90 Voir notamment les Explications du PFPDT relatives aux contrôles de sécurité (employés du secteur privé) disponible à l'adresse : www.edoeb.admin.ch/edoeb/fr/home/protection-des-donnees/

Une attention particulière doit être portée s'agissant des personnes autorisées à consulter les dossiers de candidature. Selon l'organisation d'une entreprise, ceux-ci sont susceptibles de passer en de (trop) nombreuses mains alors que seules les personnes légitimées, en général le service du personnel ou le supérieur hiérarchique, doivent y avoir accès[91].

Souvent pratiquée, la recherche d'informations personnelles liées au candidat sur un moteur de recherche[92] ou les réseaux sociaux ne sera que très rarement justifiée[93]. Une éventuelle recherche exclusivement sur un réseau social professionnel (par exemple LinkedIn) pourrait se justifier, à l'exclusion des réseaux privés (par exemple Facebook, Instagram, etc.).

A la fin du processus de recrutement, les principes de finalité et de proportionnalité impliqueront d'ailleurs un certain nettoyage dans les données traitées. Ainsi les données concernant les candidats non retenus ne devront pas être conservées, sauf accord de leur part en vue par exemple d'être contactés pour un autre poste[94].

En ce qui concerne la personne engagée, on doit aussi se poser la question de l'intérêt à conserver toutes les données liées à la candidature. Un certain nombre de ces données ne sont plus nécessaires pendant la relation de travail et devraient être détruites.

L'exemple classique est celui du contrôle des antécédents ou l'extrait de casier judiciaire. Si le candidat est engagé, c'est parce qu'il ne représente pas un risque. Cette question étant résolue, l'extrait du casier judiciaire ou le rapport détaillé des antécédents ne se justifie plus et doit être détruit. Si des exigences de contrôle interne impliquent qu'il faille prouver avoir effectué ces vérifications, une mention au dossier devrait suffire. Pour le rapport d'antécédents, la conservation des conclusions, dans certains cas, peut aussi se justifier.

arbeitsbereich/explications-relatives-aux-controles-de-securite--employes-du-se.html (consulté le 4 janvier 2021), la Directive du Conseil d'Etat vaudois LPers n° 17.2 : Conditions d'engagement – Antécédents judiciaires du 21 janvier 2004 disponible à l'adresse www.vd.ch/themes/etat-droit-finances/etat-employeur/bases-legales/directives-dapplication-du-conseil-detat/ (consulté le 4 janvier 2021), l'Ordonnance sur les contrôles de sécurité relatifs aux personnes (OCSP ; RS 120.4).

91 PFPDT, Guide 2014, p. 8.

92 On parle parfois de « googlisation ».

93 Elle se justifierait dans le cas de la recherche d'un responsable en communication ou *community manager* car la gestion de sa présence en ligne est précisément une des compétences nécessaire à son futur emploi.

94 *Ibidem*, p. 11.

Pendant la relation de travail, l'employeur va évidemment traiter un grand nombre de données personnelles du travailleur et en particulier celles qui sont nécessaires à l'exécution du contrat de travail[95], ou les données personnelles prévues par une loi[96].

L'employeur peut parfois aussi traiter des données personnelles du travailleur dans un contexte différent de celui de la relation de travail. Imaginons un travailleur qui est aussi client de l'entreprise qui l'emploie. Ces données ne sont pas liées à la relation de travail, mais bien plus au contrat de vente ou prestation. Même s'il s'agit des mêmes personnes (vendeur/employeur et acheteur/employés), les données ne doivent être mêlées. Il n'y a toutefois pas non plus une interdiction de principe de traiter les données nécessaires à la vente qui le seront de manière indépendante de la relation de travail et généralement dans des systèmes de traitement différents. L'existence de la relation de travail peut néanmoins être mentionnée dans le système de traitement des données des clients, généralement avec le consentement de l'employé (par exemple pour lui permettre de bénéficier d'un rabais s'il le souhaite). Dans certains cas cette mention reposera sur un intérêt prépondérant de l'employeur[97], par exemple dans le cas d'une banque. Si l'employé est client, il est important qu'il soit reconnaissable en tant que telle pour assurer les mesures de sécurité et de confidentialité nécessaires. Généralement la fin des relations de travail n'aura pas d'influence sur le traitement de ces données, qui pourra se poursuivre. Seule la mention de la relation de travail sera remplacée par celle d'une ancienne relation, si elle est pertinente.

V. Le traitement et la conservation de données après la fin des rapports de travail

Le droit du travail suisse ne fixe que peu d'obligations de conservation des données personnelles après la fin des relations de travail[98]. Sous l'angle du droit de la protection des données, le but du traitement qui a légitimé la conservation des données jusque-là

[95] Certaines de ces données personnelles se recoupent avec celles précédemment évoquées. Nous pouvons rajouter de manière non-exhaustive pour l'exécution du contrat de travail les données personnelles telles que le numéro AVS, les coordonnées bancaires, les certificats attestant de l'incapacité de travail de l'employé ou encore les certificats de salaire.

[96] A l'instar des éventuelles données personnelles issues d'une compensation pour perte de gain en cas de service ou en cas de maternité conformément à la Loi fédérale du 25 septembre 1952 sur les allocations pour perte de gain en cas de service et de maternité (LAPG ; RS 834.1) ou encore des données personnelles issues du versement d'une allocation familiale conformément à la Loi fédérale du 24 mars 2006 sur les allocations familiales et les aides financières allouées aux organisations familiales (LAFam ; RS 836.2) ainsi qu'aux lois cantonales d'application.

[97] Qui peut s'ajouter à celui du travailleur.

[98] Notamment les art. 46 LTr *cum* 73 OLT 1 et 13 OPTM.

disparaît le plus souvent avec la fin de la relation de travail[99]. Il n'y a plus guère de raison de traiter des données liées à l'aptitude au travail ou à l'exécution du contrat puisque celui-ci a pris fin. Tout au plus peut-on imaginer le traitement de données nécessaires à la liquidation du contrat.

Non seulement il ne se justifie plus de traiter de nouvelles données, mais le principe de proportionnalité impose même de détruire les données qui ne sont plus nécessaires. La proportionnalité temporelle limite la durée de conservation des informations à ce qui est apte et nécessaire à atteindre le but visé[100]. L'art. 6 al. 4 nLPD prévoit expressément que les données personnelles doivent être détruites ou, à tout le moins, être anonymisées dès qu'elles ne sont plus nécessaires au regard des finalités du traitement[101].

Nous verrons après quels buts peuvent être envisagés pour légitimer un traitement de données personnelles à ce stade[102], mais la fin d'une relation de travail doit aussi être vue comme une occasion de « mettre de l'ordre » dans le dossier de l'employé si, comme souvent, cela n'a pas été fait plus tôt. On comprend en effet aisément qu'il n'est guère pertinent de conserver durablement des certificats médicaux d'incapacité de travail, un courrier indiquant un changement d'adresse ou d'établissement bancaire ou encore une demande de déplacement de vacances.

L'employeur a néanmoins une obligation légale de conserver certaines données personnelles[103]. Il a ensuite le droit de conserver les données utiles à remplir ses obligations, par exemple les données nécessaires à l'établissement du certificat de travail (art. 330a CO).

L'employeur a encore le droit de conserver d'autres données lorsqu'il y a un intérêt particulier. Techniquement, il faut qu'il dispose d'un intérêt privé à conserver les données (ce qui serait une justification à violer le principe de proportionnalité et/ou de finalité), mais encore que cet intérêt prime sur celui (présumé) de l'ancien employé à ne pas subir d'atteinte à sa personnalité du fait de la conservation des données. Il n'y a pas de règle absolue et il faudra procéder dans chaque cas d'espèce à une pesée d'intérêts. Encore une fois la durée de conservation jouera un rôle important. Si l'on peut reconnaître assez

99 VERDE, p. 13.

100 Le droit suisse de la protection des données ne permet la conservation des données personnelles qu'aussi longtemps qu'elles sont nécessaires à atteindre le but visé. Cette règle émane de l'aspect de la « temporalité » qui ressort du principe de proportionnalité et est, dans le cas présent, étroitement lié au principe de la finalité (MEIER, N 679 ss.).

101 Cela découle aujourd'hui déjà du principe de la proportionnalité. Le législateur a toutefois estimé qu'il était important de le préciser explicitement, et ce notamment au vu des évolutions technologiques et des capacités (presque illimitées) de stockage (FF 2017 6645).

102 Voir chapitre VI.

103 *Cf. infra* chapitre VI.

largement un intérêt de l'employeur à conserver les données pouvant servir de preuve dans le cadre d'un litige en cours ou à venir, l'intérêt diminuera avec l'écoulement du temps. On tiendra aussi compte de la sensibilité des données. Plus elles sont sensibles, moins une longue conservation pourra se justifier.

Pour le PFPDT, seules peuvent être conservées les données indispensables telles que les données à conserver en vertu d'une obligation légale, celles dont la conservation est dans l'intérêt de l'employé (documents nécessaires à l'établissement d'un certificat de travail, par exemple) et celles dont l'employeur a besoin pour un litige pendant[104]. Comme nous le verrons, cela est un peu trop restrictif et il faut aussi admettre la conservation de données en vue d'un litige futur.

Finalement, l'employeur pourrait aussi conserver des données avec le consentement de l'ancien travailleur. On peut imaginer le cas où la fin d'un contrat de durée déterminée, le travailleur souhaite être contacté si un nouveau poste devait être disponible. Pour que l'on puisse considérer que le consentement est suffisamment libre, il devra toutefois être donné (ou confirmé) après la fin des rapports de travail.

En pratique, il est extrêmement difficile de donner une durée générale de conservation. Celle-ci dépend de chaque cas d'espèce. Pour la déterminer, il faudra d'abord se demander si le but visé n'est pas déjà atteint, puis dans le cas contraire, vérifier si les données sont toujours aptes et nécessaires à l'atteindre. Au regard de la proportionnalité au sens étroit, on s'attachera à la sensibilité et au volume de données concernées. Finalement, il sera également nécessaire de réévaluer cette durée de conservation en fonction de l'écoulement du temps. Ainsi, si la probabilité de litige diminue, l'intérêt de l'employeur à conserver les documents en lien avec l'hypothétique litige diminue également.

Le PFPDT est assez généreux puisqu'il admet une durée générale de cinq ans, voire dix ans, si la loi le prescrit[105]. Il prend appui dans ce cadre essentiellement sur le délai de prescription général de cinq ans applicable aux prétentions de l'employé issu de l'art. 128 CO. Cette approche est trop schématique à notre sens. Premièrement, la durée de cinq ans paraît (trop) longue dans de nombreux cas. Deuxièmement, si une loi prévoit la conservation, c'est bien cette durée-là qui s'applique (qu'elle soit égale, inférieure ou supérieure à dix ans)[106].

---

104 PFPDT, Guide 2014, p. 14.

105 PFPDT, Guide 2014, p. 14.

106 Et si la loi prévoit simplement un délai de prescription ou de péremption pour faire valoir une prétention, il ne se justifiera pas pour autant de conserver toujours toutes les données pouvant avoir un lien avec cette hypothétique prétention. Une certaine probabilité de la prétention et une certaine pertinence des données est au contraire nécessaire.

Finalement, et quelle que soit la durée de conservation retenue, le responsable du traitement devra adopter des mesures de sécurité supplémentaires pour les données conservées qui n'ont pas besoin d'être activement utilisées. Des restrictions d'accès doivent dès lors être mises en place : conservation séparée, clé ou mot de passe, chiffrement, etc. L'autorité française de protection des données, la Commission nationale de l'informatique et des libertés (CNIL) parle d'un statut « d'archivage intermédiaire » par opposition à celui de « base active »[107].

Ces mesures, techniques et organisationnelles, doivent apporter un niveau de protection supérieur à celles applicables aux données actives[108]. Toute mesure de protection rend l'utilisation des données moins facile et il faut habituellement trouver un équilibre entre le besoin de traiter la donnée et celui de la protéger. Dès lors que l'utilisation, et notamment la lecture, des données conservées dans un état d'archivage est rare, il est plus facile de mettre en place des mesures de sécurité plus contraignantes. A titre d'exemple, il peut être compliqué de chiffrer ou pseudonymiser les données utilisées par les employés pour enregistrer leur temps de travail car il faut qu'ils puissent y accéder facilement. En revanche, le dossier d'un ancien employé conservé dans la crainte d'une procédure peut être chiffré et nécessiter une opération plus compliquée pour pouvoir y accéder le moment venu. En outre, le nombre de personnes pouvant accéder à ces dossiers devrait être restreint et les modalités contrôlées.

VI. Quelques raisons de conserver les données après la fin des rapports de travail

A. Les données comptables

Les art. 957 ss CO imposent une obligation aux personnes morales, mais également à certaines entreprises individuelles et sociétés de personnes, de tenir une comptabilité et de présenter des comptes. Le but de cette obligation est avant tout d'enregistrer les transactions et les autres faits nécessaires à la présentation de la situation économique de l'entreprise.

La comptabilité doit être tenue selon le principe de régularité qui comprend notamment le fait de pouvoir justifier chaque enregistrement comptable par une pièce comptable[109], soit

[107] CNIL, Guide 2020, p. 5.
[108] Sur les mesures applicables en général au dossier du personnel, voir VERDE, p. 12.
[109] Art. 957a al. 2 CO.

tout document écrit, établi sur support papier, sur support électronique ou sous toute forme équivalente, qui permet la vérification de la transaction ou du fait qui est l'objet de l'enregistrement[110]. Cette obligation de tenir une comptabilité et de présenter des comptes se complète par une obligation légale de conservation. Les livres et les pièces comptables ainsi que le rapport de gestion et le rapport de révision doivent être conservés pendant une période de dix ans à compter de la fin de l'exercice comptable[111]. Les détails, notamment sur les supports admis, sont réglés dans l'Ordonnance du Conseil fédéral du 24 avril 2002 concernant la tenue et la conservation des livres de comptes[112].

Les pièces comptables contiendront régulièrement des données personnelles. Certaines données personnelles de l'ancien travailleur se retrouveront donc dans les pièces comptables que l'employeur a une obligation légale de conserver. Il peut notamment s'agir des bulletins de salaire, des preuves de versement d'une éventuelle gratification ou d'un bonus, du contrat de travail ou encore de lettres et courriels qui s'y rapportent.

Cela ne pose pas de problème sous l'angle de la protection des données, car une éventuelle atteinte à la personnalité est justifiée par la loi qui impose la conservation des données[113]. L'employeur devra néanmoins prendre garde à ne pas utiliser ces données dans un autre but que celui prévu par la loi, à savoir remplir ses obligations comptables. Il serait par exemple contraire au but (remplir ses obligations comptables) d'utiliser les bulletins de salaire pour déterminer les absences d'un employé et évaluer son taux d'absence pour renseigner un futur employeur.

B. Les registres et autres pièces

La LTr s'applique dès qu'un employeur occupe un ou plusieurs travailleurs de façon durable ou temporaire, même sans faire usage d'installations ou de locaux particuliers[114]. Parmi ses multiples obligations, l'art. 46 LTr (complété par l'art. 73 de l'Ordonnance 1 relative à la Loi sur le travail[115]) prévoit que l'employeur doit tenir à la disposition des autorités de surveillance et d'exécution les registres et autres pièces nécessaires à l'exécution de la LTr et de ses ordonnances, afin de leur permettre de s'acquitter de leurs tâches légales.

110 Art. 957a al. 3 CO.
111 Art. 958f al. 1 CO.
112 Olico ; RS 221.431. A cet égard, voir également CR CO II-TORRIONE/BARAKAT, N 1 ss *ad* art. 958f.
113 Art. 13 al. 1 LPD et 31 al. 1 nLPD.
114 Art. 1 LTr, sous réserve des exceptions des art. 2 à 4 LTr.
115 OLT 1 ; RS 822.111.

Il s'agit notamment de données concernant l'identité du travailleur et les informations liées à son contrat de travail, les données qui permettent de vérifier le respect des exigences légales en matière d'aménagement de la durée du travail et du repos, ainsi que celles en lien avec le travail de nuit et du dimanche, ainsi que de la maternité[116].

L'art. 73 al. 2 OLT 1 précise que ces registres et autres pièces doivent être conservés pendant un minimum de cinq ans à partir de l'expiration de leur validité. Concernant les documents qui contiennent des informations valables pendant une période déterminée (par exemple des fiches de salaire mensuelles ou les rapports sur les temps de travail), il est raisonnable de faire courir le délai à partir de l'expiration de la période saisie (soit la fin du mois)[117].

L'employeur n'est toutefois pas obligé de tenir ni de conserver des registres particuliers, mais il doit pouvoir présenter ces informations aux autorités sous une forme compréhensible et structurée, par exemple sur la base de documents existants (comme le contrat de travail, un registre du personnel, les décomptes horaires, les fiches de contrôle de la Suva, etc.)[118].

L'employeur a donc bien une obligation de conserver ces données pendant une durée de cinq ans, et cela indépendamment de la fin éventuelle des rapports de travail.

De manière similaire (mais concernant un nombre plus limité de travailleurs), l'art. 13 de l'Ordonnance sur la protection des travailleurs contre les risques liés aux microorganismes[119] impose à l'employeur de conserver pendant 10 ans, voire dans certains cas particuliers 40 ans[120], la liste des travailleurs ayant utilisé ou été exposés à certains microorganismes. Cette liste doit contenir l'identité des travailleurs qui sont ou ont été exposés, le type de travail effectué ainsi que, dans la mesure du possible, le microorganisme en cause, ainsi que les accidents et incidents concernés.

Le délai de conservation court à compter de la dernière utilisation de microorganismes ou la dernière exposition connue et n'est pas influencé par une éventuelle fin des rapports de travail. Si l'employeur cesse ses activités, la liste doit être remise à la Caisse nationale suisse d'assurance en cas d'accidents (SUVA)[121].

---

116 Art. 73 al. 1 OLT 1.

117 RUDOLPH, p. 39.

118 RUDOLPH, p. 39.

119 OPTM, RS 832.321.

120 Par exemple si les microorganismes en cause peuvent provoquer des infections persistantes ou latentes, que l'infection ne peut être diagnostiquée que de nombreuses années plus tard ou que l'on doit s'attendre à une période d'incubation particulièrement longue avant la déclaration de la maladie.

121 Art. 13 al. 2 et 4 OPTM.

C. Les preuves en cas de litige

Toutes les relations de travail ne se terminent pas bien et parfois le passage devant les tribunaux est inéluctable. On pense tout de suite aux cas de licenciement immédiat pour justes motifs[122] et aux cas d'abandon de poste[123], puisqu'il est assez fréquent que l'autre partie ne considère pas les motifs comme justes, mais on peut aussi ajouter les résiliations abusives[124] ou en temps inopportun[125]. Ici aussi travailleur et employeur n'ont pas toujours la même vision de la situation.

Le droit du travail fixe des délais pour ouvrir action de manière précise, par exemple un délai de 180 jours après la fin des rapports de travail en cas de résiliation considérée comme abusive[126], ou un délai de 30 jours à compter de l'abandon de l'emploi pour ouvrir action en justice ou engager des poursuites[127].

Ces délais étant assez brefs, la conservation de données personnelles pendant cette période est légitime. On ne sera pas trop strict avec le délai pour ouvrir action, puisqu'on peut y ajouter le délai raisonnable à la notification de l'action par le tribunal. Ainsi celui qui veut introduire une procédure, ou qui risque de devoir se défendre peut se prévaloir d'un intérêt légitime à la conservation des données qui sont nécessaires et aptes à prouver les prétentions qu'il allègue ou à assurer sa défense.

Il y a ensuite les cas où la relation de travail a été difficile et où l'employeur a des soupçons, par exemple de violation du devoir de fidélité ou de communication d'informations protégées par un secret. L'employeur pourrait alors envisager d'engager une procédure, indépendamment de la résiliation. Là aussi l'employeur peut faire valoir un intérêt légitime à la conservation de certaines données, pendant un certain temps. A nouveau, dans le respect du principe de proportionnalité, seules les données aptes et nécessaires à prouver les faits reprochés peuvent être conservées et la durée de conservation ne sera pas illimitée. Une conservation au-delà du délai de prescription n'est pas envisageable. Une conservation durant toute la durée délai pourrait aussi être excessive dans la majorité des cas, car plus le temps s'écoule, plus l'intérêt à engager des poursuites et donc à conserver les preuves y relatives s'amenuise. Une analyse dans chaque cas d'espèce est nécessaire et l'on ne peut pas donner de règles absolues. D'un côté si l'employeur a toutes les informations utiles et choisit de « classer l'affaire », il paraît difficile de voir un intérêt important à conserver les données. En revanche, si l'employeur dans un même cas est par

122 Art. 337 CO.
123 Art. 337d CO.
124 Art. 336 CO.
125 Art. 336c et 336d CO.
126 Art. 336b al. 1 CO.
127 Art. 337d al. 4 CO, sous réserve de compensation.

exemple convaincu que le travailleur a violé certaines de ses obligations et dispose des informations pour le prouver, mais qu'il choisit de ne pas engager de poursuites par opportunité considérant qu'il n'est pas impacté tant que le travailleur ne lui fait pas de concurrence directe, on pourrait alors admettre un intérêt légitime à la conservation des données nécessaires dans le cas où l'ancien travailleur viendrait à agir de manière à créer une concurrence directe. Plus la probabilité est grande, plus l'intérêt à conserver les données est légitime.

Si le travailleur a fait régulièrement des reproches ou formulé des demandes pouvant prendre la forme de prétentions en justice, l'employeur pourra aussi faire valoir un intérêt à conserver des données pertinentes pour s'y opposer. Plus le temps passe, plus la probabilité d'une action diminue et donc également l'intérêt à conserver des données.

On peut encore mentionner le cas d'obligations particulières du travailleur, comme un engagement de confidentialité ou une prohibition de concurrence. Dans ce cas non seulement l'employeur a un intérêt prépondérant à conserver certaines données utiles à prouver une violation de ces engagements, mais il peut aussi avoir un intérêt à traiter de nouvelles données pour vérifier le respect des engagements pris. Comme toujours, le traitement de données devra être proportionné au but visé. A titre d'exemple, on peut mentionner une observation de l'activité sur LinkedIn. Une alerte par mots-clés scannant les pages web serait au contraire disproportionnée, notamment parce qu'elle impliquerait de nombreuses données sans lien avec le but visé et violerait également l'art. 328b CO[128].

Finalement, il y a le cas où l'employeur n'envisage pas de prétentions (fondées ou non) du travailleur. Dans cette dernière hypothèse, une approche très prudente de l'employeur pourrait le conduire à vouloir conserver pendant un certain temps certaines données importantes. Cela n'est *a priori* pas exclu, mais il faudrait néanmoins des éléments particuliers liés au cas d'espèce. Une conservation systématique jusqu'à l'échéance du délai de prescription serait dans tous les cas excessive (que l'on retienne un délai de prescription de 20 ans pour des lésions corporelles[129] ou celui de 5 ans pour les prestations contractuelles des travailleurs)[130].

D. Le cas de la non-embauche

A la fin du processus de recrutement, il n'y a plus guère de justifications à conserver les données personnelles des candidats non retenus, et elles seront supprimées, sauf accord de

[128] On peut se référer *mutatis mutandis* aux art. 57m LOGA et PFPDT, Guide 2014.
[129] Art. 60 al. 1bis CO.
[130] Art. 128 CO.

leur part en vue par exemple d'un autre poste[131]. On peut néanmoins admettre la conservation de la lettre de postulation ainsi qu'une liste des personnes ayant postulé pour pouvoir identifier des candidatures récurrentes ou en cas de réclamation de la part d'un candidat non retenu[132].

Le PFPDT semble plutôt s'attacher à l'origine du document et considère que les documents soumis par les personnes dont la candidature a été écartée doivent leur être restitués à l'issue de la procédure de sélection (et les copies, s'il en existe, détruites immédiatement) et que l'employeur ne peut conserver que les documents qui lui appartiennent, c'est-à-dire les lettres de candidature, les questionnaires du personnel, les tests graphologiques et les renseignements recueillis à la suite de demandes de référence. Le PFPDT précise néanmoins que ces documents et renseignements, de même que les données relatives à la santé, doivent être détruits[133].

Si les données doivent être retournées ou détruites, cela ne doit pas obligatoirement se faire le jour de la décision de non-embauche. La Loi fédérale sur l'égalité entre femmes et hommes (LEg) prévoyant un délai de trois mois dès la notification de non-embauche pour faire valoir des prétentions[134], une conservation pendant trois mois et quelques jours est parfaitement légitime.

Pour le personnel de la Confédération, la question est expressément réglée dans l'Ordonnance fédérale du 22 novembre 2017 concernant la protection des données personnelles du personnel de la Confédération[135] qui prévoit pour les candidats non retenus à un emploi au sein de l'administration fédérale que les dossiers de candidature transmis sur papier leur sont renvoyés. Les autres données, à l'exception de la lettre de candidature, sont détruites au plus tard dans les trois mois suivant la clôture de la procédure de candidature[136]. Pour les candidatures électroniques, les données sont détruites au plus tard trois mois après la clôture de la procédure de candidature[137].

---

131 Dans le même sens, GT 29, Avis 2/2017, p. 12 : « les données recueillies au cours du processus de recrutement devraient en principe être effacées dès qu'il devient clair que la candidature ne sera pas retenue par l'employeur ou sera retirée par le candidat. » Voir également l'art. 13.2 de la Recommandation CM/Rec (2015) 5 du Comité des Ministres aux Etats membres sur le traitement des données à caractère personnel dans le cadre de l'emploi du 1er avril 2015.

132 On peut penser ici à une action en application de la Loi sur l'égalité (LEg ; RS 151.1), voir ci-après.

133 PFPDT, Guide 2014, p. 11.

134 Art. 8 al. 2 LEg.

135 OPDC ; RS 172.220.111.4.

136 Art. 10 al. 3 OPDC.

137 Art. 18 OPDC.

E. Les assurances sociales

Pendant la relation de travail, l'employeur doit assumer de nombreuses obligations prévues par les différences assurances, sociales et privées[138]. Cela inclut le traitement de données personnelles souvent « sensibles », puisqu'en lien avec l'état de santé des personnes[139], ainsi que leur communication à des autorités en charge de l'application du droit des assurances sociales.

Si le traitement des données par les assurances sociales fait l'objet de règles précises[140], ce n'est pas tellement le cas pour l'employeur. En l'absence de règle obligeant l'employeur à conserver des données, il peut néanmoins avoir un intérêt prépondérant à conserver les données personnelles liées à des prétentions possibles, qu'il s'agisse des siennes, de celles du travailleur ou de l'assurance sociale.

A cet égard, on peut mentionner l'art. 24 al. 1 LPGA qui prévoit que le droit à des prestations ou à des cotisations arriérées s'éteint cinq ans après la fin du mois pour lequel la prestation était due et cinq ans après la fin de l'année civile pour laquelle la cotisation devait être payée. Une conservation pendant cette durée pourrait se justifier pour les données personnelles connexes à l'existence d'un droit à une prestation découlant des assurances sociales comme cela a été dit précédemment s'agissant des preuves en cas de litige. Au surplus, la plupart des documents intéressants concerneront la fixation des cotisations ou des prestations et seront déjà couverts par l'obligation de conservation de dix ans applicable aux pièces comptables.

---

138 Telles que l'assurance-maladie, l'assurance-accidents, l'assurance-chômage, l'assurance-vieillesse et survivants ou encore l'assurance-invalidité, l'assurance perte de gain, etc.

139 DUPONT, p. 195.

140 Lors de l'adaptation et l'harmonisation des bases légales pour le traitement de données personnelles dans les assurances sociales, le législateur a fait le choix d'intégrer individuellement à chaque loi d'assurance sociale une disposition générale formant la base légale des traitements (FF 2000 224-225). C'est le cas des art. 85a ss LPP, 49a ss LAVS, 66 ss LAI, 29 ss LAPG. Malgré tout, ces dispositions légales n'ancrent pas en leur sein la durée de la conservation exacte des données traitées. Le message du Conseil fédéral rappelle à ce propos que le principe de la proportionnalité, qui régit tout le droit administratif, exige en particulier que le nombre et la nature des données personnelles recueillies, le flux de ces données et la durée de leur conservation se limitent à ce qui est nécessaire à l'accomplissement des tâches légales. Il y a toutefois lieu de souligner que l'Office fédéral des assurances sociales a adopté des Directives du 1er janvier 2011 sur la gestion des dossiers dans les domaines AVS/AI/APG/PC/AfamAgr/Afam. Ces directives prévoient notamment que les dossiers doivent être conservés jusqu'à dix ans après l'extinction du dernier droit à prestation et que la destruction du dossier ne peut intervenir qu'à la condition qu'ils ne soient plus nécessaires pour des prestations pouvant être octroyées ultérieurement (voir notamment les N 1602 et 1603). Partant, la durée de conservation semble particulièrement longue.

F. Le certificat de travail et les références

Selon l'art. 330a CO, le travailleur a, en tout temps, la possibilité de demander à son employeur un certificat de travail portant sur la nature et la durée des rapports de travail, ainsi que sur la qualité de son travail et sa conduite. Le travailleur peut également exiger de l'employeur que le certificat ne puisse porter que sur la nature et la durée des rapports de travail. La loi distingue ainsi deux types de certificats, soit le certificat détaillé (art. 330a al. 1 CO) et le certificat simple (art. 330a al. 2 CO), mais dans un cas comme dans l'autre, son importance est considérable[141].

Indépendamment de la forme du certificat de travail, il s'agit d'un document apprécié par tout employeur dans le cadre d'un processus de recrutement. Ce dernier est censé permettre par sa simple lecture d'identifier les qualités d'un candidat et d'évaluer ses capacités professionnelles, permettant ainsi à un nouvel employeur de procéder à une première sélection parmi plusieurs candidats[142]. Il joue donc un rôle essentiel, à la fois pour le travailleur comme pour l'employeur, réciproquement dans la recherche d'un nouvel emploi ou dans la recherche d'un nouveau candidat.

Il incombe à chaque employeur de rédiger un certificat de travail lorsqu'un collaborateur ou ancien collaborateur en fait la demande. Le contenu du certificat de travail doit répondre à certains principes, à savoir que ce contenu se doit notamment d'être objectif, bienveillant et exact[143]. Lors de l'établissement d'un certificat de travail simple, l'employeur doit uniquement indiquer la nature des rapports de travail ainsi que sa durée. Outre ces points, le certificat doit évidemment permettre l'identification de l'ancien employé. Ainsi, tel que rédigé, le certificat simple devrait vraisemblablement contenir le nom, le prénom, la nature de l'emploi[144] ainsi que sa durée. Dans le cadre d'un certificat détaillé, l'employeur doit en plus indiquer son appréciation sur la qualité du travail ainsi que sur la conduite du travailleur. Un tel certificat indique dès lors en sus les capacités professionnelles de l'ancien employé et son aptitude à exercer le métier en cause[145].

---

141 WYLER/HEINZER, pp. 523 ss ; CR CO I-AUBERT, N 1 ss *ad* art. 330a ; MARTIN ANTIPAS, p. 2 ; AUBERT, *in* : Dunand/Mahon, N 1 ss *ad* art. 330a CO.

142 MARTIN ANTIPAS, pp. 2-3.

143 WYLER/HEINZER, pp. 523-528 ; CR-CO-AUBERT, N 4 *ad* art. 330a ; MARTIN ANTIPAS, pp. 11-13 ; AUBERT, *in* : Dunand/Mahon, N 16-20 *ad* art. 330a CO.

144 A savoir la fonction exacte du travail ainsi que ses éventuelles responsabilités ou tâches particulières. *Cf.* AUBERT, *in* : Mahon/Pascal, N 22 *ad* art. 330a CO.

145 AUBERT, *in* : Mahon/Pascal, N 25-30 *ad* art. 330a CO ; MARTIN ANTIPAS, pp. 18-20. En tant que telles, les données relatives aux capacités professionnelles se doivent d'être considérées comme des données personnelles au sens de la LPD.

Si le travailleur a en tout temps l'occasion de demander un certificat de travail à son employeur, dans les faits, le moment où celui-ci est la plupart du temps demandé est à l'approche de la fin d'une relation contractuelle de travail. Dans ce cadre, et au vu de ce qui précède, l'employeur dispose d'un intérêt privé à conserver les données personnelles nécessaires à la rédaction éventuelle du certificat de travail ou, subsidiairement, en cas de potentielle contestation par le travailleur à l'encontre d'un précédent certificat de travail intermédiaire ou de tout autre document contenant une évaluation professionnelle faite par l'employeur[146]. Nous pensons ici notamment aux comptes-rendus d'entretiens d'évaluation.

La conservation des données ne doit cependant pas intervenir « pour le cas où », notamment avec en tête l'idée d'être « consulté » par de futurs employeurs sur le travailleur en question. Ainsi, une fois rédigé, l'employeur devrait supprimer les données qui étaient uniquement nécessaires à la rédaction d'un certificat de travail et conserver à la place ce dernier. Un employé a dix ans depuis la fin des rapports de travail pour exiger la fourniture d'un certificat de travail. Les données nécessaires à sa rédaction doivent donc être conservées pendant toute cette durée afin de permettre à l'employeur de pouvoir respecter son obligation légale le cas échéant.

Se pose encore la question de la prise de références par un futur employeur potentiel auprès de précédents employeurs. A cet égard, le potentiel employeur se doit d'avoir le consentement exprès du candidat avant de procéder à toute demande de références. Le consentement du candidat peut ressortir de son dossier de candidature lorsque ce dernier contient expressément les coordonnées d'une personne de référence et que cette dernière est indiquée comme telle[147]. A ceci s'ajoute le fait que les précédents employeurs ne peuvent donner aucun renseignement sans y avoir été autorisés par le travailleur[148]. Cette autorisation peut découler d'une demande générale de la part de l'ancien employé d'être cité comme référence dans son dossier de candidature ou il peut s'agir d'une autorisation spécifique à une postulation en particulier.

VII. Quelques considérations pratiques

Même si les principes sont relativement clairs, il faut bien admettre que la situation en pratique est souvent assez compliquée. Il est en effet plutôt rare que les données soient

146 Eventuelle car il appartient au travailleur de demander à son employeur de rédiger un tel certificat. Sa rédaction n'est pas automatique.

147 Une simple mention du nom de son ancien responsable n'est par exemple pas suffisante.

148 Dans le même sens, voir CARRUZZO, N 8 *ad* art. 328b CO.

naturellement séparées et triées et que l'on puisse aisément supprimer un répertoire de données en bloc et en conserver un autre.

Pour les données dont la conservation est obligatoire, la situation est parfois un peu meilleure. C'est en particulier le cas des données comptables[149], car l'employeur est habitué à les traiter en dehors du dossier du personnel.

On pourrait s'attendre à ce que ce soit aussi le cas pour les registres et autres pièces[150] (VI.B), à tout le moins pour une partie de ces données. La réalité dépendra beaucoup de la taille de l'entreprise et de son domaine d'activité. Les employeurs soumis à l'OPTM tiennent certainement un registre séparé pour ces informations. Ce ne sera en revanche pas toujours le cas pour les obligations de l'art. 73 OLT 1 puisque précisément ces informations peuvent soit figurer dans un registre (ce qui est plus compliqué au moment de son établissement mais plus simple pour sa conservation) soit dans des documents épars et variés.

Si le registre est tenu de manière informatisée, il est assez facile de prévoir dès l'enregistrement des informations une date de suppression automatique (ou pour une variante moins radicale une alerte automatique à valider avant d'engager la suppression). Pour les registres papier, ou les registres électroniques plus basiques, une suppression manuelle et régulière s'impose.

Il y a ensuite souvent un dossier nominal par employé, parfois une ou plusieurs versions papier et électroniques. La nature des données contenues varie beaucoup, parfois avec des sous-dossiers. L'employeur n'échappera pas au tri de son contenu.

Pour toutes les données qui ne figurent pas dans la comptabilité ou un dossier dédié, il faut bien se rendre compte que c'est uniquement la nature et le contenu du document et des données personnelles qui détermineront son intérêt à la conservation, et cas échéant sa durée. Ce ne sera ni son format, ni le lieu où il se trouve[151].

L'employeur, en qualité de responsable du traitement, doit donc procéder à une classification des données personnelles en sa possession et des documents contenant de telles données personnelles. Au départ de l'employé[152], un tri est donc nécessaire, et pour chaque donnée personnelle, ou chaque document, le responsable du traitement doit se demander si la conservation est nécessaire. Cela concerne autant le dossier papier de

149 Voir VI.A ci-dessus.

150 Voir VI.B ci-dessus.

151 Cela surprend souvent les informaticiens, qui partent du système d'information pour identifier son contenu, et qui souhaitent pouvoir programmer des durées de suppression par système.

152 Mais aussi régulièrement pendant la durée des rapports de travail.

l'employé que les versions électroniques, les dossiers de candidature, les documents remis ou encore la correspondance.

L'employeur ne peut pas se contenter de respecter la LPD et la personnalité de ses travailleurs qu'à leur départ. Bien plus, il doit s'assurer tout au long des rapports de travail que seules les données qui doivent ou peuvent être conservées le sont. Cela implique d'établir des lignes directrices relatives à la classification des données, leur durée de conservation, les droits d'accès et les personnes responsables. Pour certaines données il est possible de fixer une durée de conservation dès leur enregistrement, alors que pour d'autres ce sera la réalisation d'un événement (par exemple un accident, un licenciement, etc.) qui déterminera le point de départ de la durée.

Pour les petites entreprises, en tenant compte des risques et des moyens disponibles, on devrait admettre un tri manuel des dossiers, par exemple une fois par année et au départ des travailleurs. Une stricte limitation des accès aux données est néanmoins nécessaire.

On se rend également bien compte que la messagerie électronique est un casse-tête, à tout le moins telle qu'elle est actuellement exploitée. Si l'on pense au courrier papier, tout document reçu par un collaborateur est lu puis classé là où il est nécessaire, éventuellement détruit s'il n'est pas pertinent. Il ne viendrait à personne l'idée de conserver sur son bureau, pendant des années, des copies de toutes les lettres reçues et envoyées. Et personne n'aurait l'idée d'y ajouter tous les messages vocaux laissés et reçus, les notes et post-its insignifiants, les brouillons et documents supprimés.

Pourtant il faut bien admettre que c'est ce que la plupart des employés font avec leur messagerie électronique. D'un canal de communication temporaire (une boîte aux lettres), la messagerie est devenue un dépôt, plus ou moins gérée et, ce qui est plus grave, plus ou moins nécessaire, pour des informations qui sont tantôt utiles, tantôt futiles, tantôt exclusivement dans la messagerie, tantôt également enregistrées ailleurs. Il reste donc deux options pour gérer une telle messagerie : reprendre régulièrement chaque message un à un pour décider s'il doit ou non être conservé[153], ou tout supprimer[154].

Avant d'en arriver là, la seule vraie solution consiste probablement à imposer à chaque collaborateur (et lui donner les moyens) de classer les éléments importants hors de la messagerie, qu'il s'agisse de dossiers physiques ou électroniques, ou d'un outil de gestion de documents. Ainsi une suppression automatique des courriels est possible par exemple après douze mois. Cela permet de s'assurer que les données personnelles d'un ancien

[153] Efficace mais difficilement envisageable quand on a quelques dizaines de milliers de messages.

[154] Beaucoup plus simple mais pas sans risque si les informations et documents n'ont pas été sauvegardés ailleurs. Une variante un peu moins brutale consiste à archiver les données de manière chiffrée pendant une période intermédiaire pour limiter les risques.

travailleur dont la conservation n'est pas justifiée ne demeurent pas dans les messageries de ses collègues. Quant à la messagerie de l'ancien travailleur, elle doit évidemment être désactivée[155].

En conclusion, il faut retenir que c'est déjà au moment de la collecte des données personnelles qu'il faut envisager la durée de leur conservation[156]. En les classant au bon endroit, voire en prévoyant dès le début la durée de conservation, le travail n'en sera que plus simple. Et dans tous les cas au moment du départ d'un travailleur, l'employeur doit faire un tri dans le dossier de l'ancien travailleur, mais également dans les autres dossiers et systèmes pouvant contenir des données le concernant.

[155] Sur cette question, voir par exemple MÉTILLE, Surveillance, pp. 122-123.

[156] La nLPD prévoit d'ailleurs que cette durée figure dans le registre des traitements (art. 12 nLPD) et dans la réponse à un droit d'accès (art. 25 nLPD). Le RGPD va encore plus loin et en fait une information à fournir lors de la collecte (art. 13 RGPD).

Bibliographie

Sauf indication contraire, les ouvrages ou articles de cette bibliographie sont cités dans les notes avec l'indication du seul nom de l'auteur.

A. Littérature juridique

BELSER EVA MARIA/EPINEY ASTRID/WALDMANN BERNHARD (édit.), Datenschutzrecht – Grundlagen und öffentliches Recht, Berne 2011 (cité : AUTEUR, *in :* Belser/Epiney/Waldmann).

CARRUZZO PHILIPPE, Le contrat individuel de travail – Commentaire des articles 319 à 341 du Code des obligations, Zurich 2009.

DUNAND JEAN-PHILIPPE/MAHON PASCAL (édit.), Commentaire du contrat de travail, Berne 2013 (cité : AUTEUR, *in* : Dunand/Mahon).

DUPONT ANNE-SYLVIE, La protection des données confiées aux assureurs, *in :* Dunand Jean-Philippe/Mahon Pascal (édit.), La protection des données dans les relations de travail, Genève/Zurich/Bâle 2017, pp. 195 ss.

MARTIN ANTIPAS FRANÇOISE, Certificats de travail, *in* : Dunand Jean-Philippe/Mahon Pascal, Les certificats dans les relations de travail (édit.), Zurich 2018.

MAURER-LAMBROU URS/BLECHTA GABOR-PAUL (édit.), Datenschutzgesetz (DSG)/Öffentlichkeitsgesetz (BGÖ), Basler Kommentar, 3e éd., Bâle 2014 (cité : BSK DSG-AUTEUR).

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

MEIER PHILIPPE/TSCHUMY NICOLAS, L'adresse IP : une donnée personnelle ? Ou quand la CJUE rejoint le TF !, *in* : Jusletter du 23 janvier 2017.

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

MÉTILLE SYLVAIN, Internet et droit, Zurich 2017 (cité : MÉTILLE, Internet et droit).

RAEDLER DAVID, Les enquêtes internes dans un contexte suisse et américain : instruction de l'entreprise ou Cheval de Troie de l'autorité ?, Lausanne 2018.

ROSENTHAL DAVID, Das neue Datenschutzgesetz, *in :* Jusletter du 16 novembre 2020.

ROSENTHAL DAVID/JÖHRI YVONNE, Handkommentar zum Datenschutzgesetz, Zurich 2008.

RUDOLPH ROGER, L'obligation d'enregistrement de la durée du travail selon la nouvelle réglementation, TREX 2016, pp. 38 ss.

TAMÒ-LARRIEUX AURELIA, Designing for Privacy and its Legal Framework – Data Protection by Design and Default for the Internet of Things, Cham 2018.

TERCIER PIERRE/AMSTUTZ MARC/TRIGO TRINDADE RITA (édit.), Commentaire romand – Code des obligations II, 2e éd., Bâle 2017 (cité : CR CO II-AUTEUR).

THÉVENOZ LUC/WERRO FRANZ (édit.), Commentaire romand – Code des obligations I, 2e éd., Bâle 2012 (cité : CR CO I-AUTEUR).

VERDE MICHEL, Rechtliche Aspekte der Personalakte, *in* : Jusletter du 10 août 2020.

WYLER RÉMY/HEINZER BORIS, Droit du travail, 4e éd., Berne 2019.

B. Documents officiels

CONSEIL FÉDÉRAL, Message du 15 septembre 2017 concernant la loi fédérale sur la révision totale de la loi fédérale sur la protection des données et la modification d'autres lois fédérales, FF 2017, pp. 6565 ss.

CONSEIL FÉDÉRAL, Message du 24 novembre 1999 concernant l'adaptation et l'harmonisation des bases légales pour le traitement de données personnelles dans les assurances sociales, FF 2000, pp. 219 ss.

CONSEIL FÉDÉRAL, Rapport du 9 décembre 2011 sur l'évaluation de la loi fédérale sur la protection des données, FF 2012, pp. 265 ss.

COMITÉ EUROPÉEN DE LA PROTECTION DES DONNÉES, Guidelines 4/2019 on Article 25 Data Protection by Design and by Default, version 2.0 adoptées le 20 octobre 2020 (uniquement disponible en anglais pour le moment).

COMITÉ EUROPÉEN DE LA PROTECTION DES DONNÉES, Guidelines 07/2020 on the concepts of controller and processor in the GDPR, version 1.0 adoptées le 2 septembre 2020 (uniquement disponible en anglais pour le moment).

OFFICE FÉDÉRAL DES ASSURANCES SOCIALES, Directives du 1er janvier 2011 sur la gestion des dossiers dans les domaines AVS/AI/APG/PC/AfamAgr/Afam.

PRÉPOSÉ FÉDÉRAL À LA PROTECTION DES DONNÉES ET À LA TRANSPARENCE, Guide d'octobre 2014 pour le traitement des données personnelles dans le secteur du travail – Traitement par des personnes privées (cité : PFPDT, Guide 2014).

COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS, Guide pratique de juillet 2020 – Les durées de conservation (cité : CNIL, Guide 2020).

GROUPE DE TRAVAIL « ARTICLE 29 » SUR LA PROTECTION DES DONNÉES, Avis 2/2017 sur le traitement des données sur le lieu de travail (cité : GT 29, Avis 2/2017).