La protection des données dans les relations de travail

Jean-Philippe Dunand
Pascal Mahon

Volume 10

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

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

© Schulthess Médias Juridiques SA, Genève · Zurich · Bâle 2017

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

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

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

Avant-propos

Chaque employeur collecte, conserve et communique de nombreuses données concernant ses employés. Le développement fulgurant des nouvelles technologies a augmenté les risques d'atteinte à la personnalité des employés et à la sécurité des données. À n'en pas douter, la protection des données dans les relations de travail est un thème de grande actualité auquel les employés et les employeurs sont de plus en plus sensibles. Les juristes et avocats y sont eux-mêmes confrontés de manière croissante.

En date du 21 décembre 2016, le Conseil fédéral a mis en consultation un avant-projet de révision totale de la législation en matière de protection des données. Dans la foulée, un colloque a été organisé le 17 mars 2017 à l'Université de Neuchâtel, conjointement par la Chambre neuchâteloise du commerce et de l'industrie (CNCI) et le Centre d'étude des relations de travail (CERT), pour tenter de répondre aux principales questions juridiques concernant la protection des données dans les relations de travail. Cet ouvrage comprend les actes du colloque sous la forme de treize articles rédigés par des contributrices et contributeurs suisses romands, actifs dans l'enseignement et/ou la pratique du droit du travail et du droit de la protection des données.

Nos vifs remerciements vont en premier lieu aux auteur-e-s qui ont rédigé des contributions de qualité malgré leur emploi du temps chargé. Ils s'adressent aussi à Mesdames Lilla Balázs (étudiante en droit à l'Université de Neuchâtel), Joanna David (cheffe de projet auprès de Schulthess éditions romandes), Anouk Gillabert (collaboratrice administrative à l'Université de Neuchâtel) et Sylvia Staehli (assistante de direction à l'Université de Neuchâtel), pour leur collaboration diligente et appréciée à la confection de l'ouvrage.

Neuchâtel, mars 2017

Prof. Jean-Philippe Dunand

Co-directeur du CERT

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

Table des abréviations

Abs.	Absatz
ad	à
AI	Assurance-invalidité
AJP	Aktuelle Juristische Praxis
al.	alinéa(s)
AP	Avant-projet
APC	Association du personnel de la Confédération
ArbG	Arbeitsgericht
art.	article(s)
Art.	Artikel
ASEB	Association suisse des employés de banque
ATAF	Recueil officiel des arrêts du Tribunal administratif fédéral
ATF	Recueil officiel des arrêts du Tribunal fédéral suisse
ats	Agence Télégraphique Suisse
ATSG	Bundesgesetz über den Allgemeinen Teil des Sozialversicherungsrechts vom 6. Oktober 2000, SR 830.1
AVG	Bundesgesetz über die Arbeitsvermittlung und den Personalverleih (Arbeitsvermittlungsgesetz) vom 6. Oktober 1989, SR 823.11
AVS	Assurance-vieillesse et survivants
BCM	Business Continuity Management (gestion de la continuité de l'activité)
BCR	Binding Corporate Rules (règles d'entreprise contraignantes)
BGÖ	Bundesgesetz über das Öffentlichkeitsprinzip der Verwaltung (Öffentlichkeitsgesetz) vom 17. Dezember 2004, SR 152.3
BPG	Bundespersonalgesetz vom 24. März 2000, SR 172.220.1
BV	Bundesverfassung der Schweizerischen Eidgenossenschaft vom 18. April 1999, SR 101
BV-PLUS	Système d'information concernant le personnel de l'administration fédérale
BYOD	Bring Your Own Device (AVEC, Apportez votre équipement personnel de communication)
c.	considérant(s)
c.	contre
c.à.d.	c'est-à-dire
CAPH	Cour d'appel des prud'hommes
CC	Code civil suisse du 10 décembre 1907, RS 210
CCRA	Convention collective sur la retraite anticipée
CCT	Convention collective de travail

CEDH	Convention de sauvegarde des droits de l'homme et des libertés fondamentales du 4 novembre 1950, RS 0.101
CEDIDAC	Centre du droit de l'entreprise, Université de Lausanne
cf.	confer
CFF	Chemins de fer fédéraux
CFV	Commission fédérale pour les vaccinations
CGA	Conditions générales d'assurance
ch.	chiffre(s)
CII	Collaboration interinstitutionnelle
CJ	Cour de justice
CJUE	Cour de justice de l'Union européenne
CNIL	Commission nationale de l'informatique et des libertés (France)
CO	Loi fédérale complétant le Code civil suisse (Livre cinquième : Droit des obligations) du 30 mars 1911, RS 220
COMCO	Commission de la concurrence
Convention STE 108	Convention du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel du 28 janvier 1981
CourEDH	Cour européenne des droits de l'homme
CP	Code pénal suisse du 21 décembre 1937, RS 311.0
CP	Commission paritaire
CPC	Code de procédure civile du 19 décembre 2008, RS 272
CPDT-JUNE	Convention intercantonale relative à la protection des données et à la transparence dans les cantons du Jura et de Neuchâtel, RSN 150.30
CPP	Code de procédure pénale suisse du 5 octobre 2007, RS 312.0
CRCT	Chambre des relations collectives de travail du canton de Genève
Cst.	Constitution fédérale de la Confédération suisse du 18 avril 1999, RS 101
DEFR	Département fédéral de l'économie, de la formation et de la recherche
DFF	Département fédéral des finances
DFI	Département fédéral de l'intérieur
DFJP	Département fédéral de justice et police
DLP	Data Loss Prevention (prévention des pertes de données)
DPA	Loi fédérale sur le droit pénal administratif du 22 mars 1974, RS 313.0
DPD	Délégué à la protection des données
DRG	Diagnosis Related Group
DRM	Digital Rights Management (Gestion des droits numériques ou électroniques)
DSG	Bundesgesetz über den Datenschutz vom 19. Juni 1992, SR 235.1
DTA	Revue de droit du travail et d'assurance-chômage
éd./éds.	éditeur/éditeurs

EEE	Espace économique européen
ég.	également
et al.	et les autres personnes
FF	Feuille fédérale
FINMA	Autorité fédérale de surveillance des marchés financiers
FlaM	Flankierende Massnahmen (mesures d'accompagnement)
FMH	Fédération des médecins suisses
GIG	Bundesgesetz über die Gleichstellung von Frau und Mann (Gleichstellungsgesetz) vom 24. März 1995, SR 151.1
GPS	Global Positioning System (système de positionnement mondial)
HAVE	Haftung und Versicherung (Zeitschrift)
HCDH	Haut-Commissariat des Nations Unies aux droits de l'homme
IA	Intelligence artificielle
ibid./*ibidem*	au même endroit
IEC	International Electrotechnical Commission (Commission électrotechnique internationale)
i.f./*in fine*	à la fin
IIZ	Interinstitutionnelle Zusammenarbeit
infra	plus bas
IRAL	Institut du droit des assurances et du travail, Université de Lausanne
ISO	International Organisation for Standardization (Organisation internationale de normalisation)
JAAC	Jurisprudence des autorités administratives de la Confédération
JAR	Jahrbuch des Schweizerischen Arbeitsrechts
JdT	Journal des Tribunaux
JO	Journal officiel de l'Union européenne
JORF	Journal officiel de la République française
LAA	Loi fédérale sur l'assurance-accidents du 20 mars 1981, RS 832.20
LaCC	Loi genevoise d'application du code civil suisse et d'autres lois fédérales en matière civile du 11 octobre 2012, RS/GE E1 05
LACI	Loi fédérale sur l'assurance-chômage obligatoire et l'indemnité en cas d'insolvabilité (Loi sur l'assurance-chômage) du 25 juin 1982, RS 837.0
LAFam	Loi fédérale sur les allocations familiales (Loi sur les allocations familiales) du 24 mars 2006, RS 836.2
LAGH	Loi fédérale sur l'analyse génétique humaine du 8 octobre 2004, RS 810.12
LAI	Loi fédérale sur l'assurance-invalidité du 19 juin 1959, RS 831.20
LAM	Loi fédérale sur l'assurance militaire du 19 juin 1992, RS 833.1
LAMal	Loi fédérale sur l'assurance-maladie du 18 mars 1994, RS 832.10

LAPG	Loi fédérale sur les allocations pour perte de gain en cas de service et de maternité (Loi sur les allocations pour perte de gain) du 25 septembre 1952, RS 834.1
LAr	Loi fédérale sur l'archivage du 26 juin 1998, RS 152.1
LAVS	Loi fédérale sur l'assurance-vieillesse et survivants du 20 décembre 1946, RS 831.10
LB	Loi fédérale sur les banques et les caisses d'épargne (Loi sur les banques) du 8 novembre 1934, RS 952.0
LCA	Loi fédérale sur le contrat d'assurance (Loi sur le contrat d'assurance) du 2 avril 1908, RS 221.229.1
LCal	Loi fédérale sur le commerce des boissons alcooliques (Loi sur le commerce de l'alcool), (RS 680, pas en vigueur)
LCart	Loi fédérale sur les cartels et autres restrictions à la concurrence (Loi sur les cartels) du 6 octobre 1995, RS 251
LCD	Loi fédérale contre la concurrence déloyale du 19 décembre 1986, RS 241
LDA	Loi fédérale sur le droit d'auteur et les droits voisins (Loi sur le droit d'auteur) du 9 octobre 1992, RS 231.1
LDét	Loi fédérale sur les mesures d'accompagnement applicables aux travailleurs détachés et aux contrôles des salaires minimaux prévus par les contrats-types de travail (Loi sur les travailleurs détachés) du 8 octobre 1999, RS 823.20
LECCT	Loi fédérale permettant d'étendre le champ d'application de la convention collective de travail du 28 septembre 1956, RS 221.215.311
LEg	Loi fédérale sur l'égalité entre femmes et hommes du 24 mars 1995, RS 151.1
let./lit.	lettre(s)
LEtr	Loi fédérale sur les étrangers du 16 décembre 2005, RS 142.20
LFus	Loi fédérale sur la fusion, la scission, la transformation et le transfert de patrimoine (Loi sur la fusion) du 3 octobre 2003, RS 221.301
LGVE	Luzerner Gerichts- und Verwaltungsentscheide
LHand	Loi fédérale sur l'élimination des inégalités frappant les personnes handicapées (Loi sur l'égalité pour les handicapés) du 13 décembre 2002, RS 151.3
LHID	Loi fédérale sur l'harmonisation des impôts directs des cantons et des communes du 14 décembre 1990, RS 642.14
LIPDA	Loi vaudoise sur l'information du public, la protection des données et l'archivage du 9 octobre 2008, RSV 170.2
LOGA	Loi sur l'organisation du gouvernement et de l'administration du 21 mars 1997, RS 172.010
LOST	Loi fédérale sur les organes de sécurité des entreprises de transports publics du 18 juin 2010, RS 745.2
LPD	Loi fédérale sur la protection des données du 19 juin 1992, RS 235.1
LPers	Loi fédérale sur le personnel de la Confédération du 24 mars 2000, RS 172.220.1

LPGA	Loi fédérale sur la partie générale du droit des assurances sociales du 6 octobre 2000, RS 830.1
LPP	Loi fédérale sur la prévoyance professionnelle vieillesse, survivants et invalidité du 25 juin 1982, RS 831.40
LRens	Loi fédérale sur le renseignement, (RS 121, pas en vigueur)
LSE	Loi fédérale sur le service de l'emploi et la location de services du 6 octobre 1989, RS 823.11
LSt	Loi neuchâteloise sur le statut de la fonction publique du 28 juin 1995, RSN 152.510
LTAE	Loi neuchâteloise sur la transparence des activités étatiques du 28 juin 2006, RSN 150.50
LTAF	Loi sur le Tribunal administratif fédéral du 17 juin 2005, RS 173.32
LTF	Loi sur le Tribunal fédéral du 17 juin 2005, RS 173.110
LTN	Loi fédérale concernant des mesures en matière de lutte contre le travail au noir (Loi sur le travail au noir) du 17 juin 2005, RS 822.41
LTP	Loi neuchâteloise sur les transports publics du 1er octobre 1996, RSN 765.1
LTr	Loi fédérale sur le travail dans l'industrie, l'artisanat et le commerce (Loi sur le travail) du 13 mars 1964, RS 822.11
LTrans	Loi fédérale sur le principe de la transparence dans l'administration (Loi sur la transparence) du 17 décembre 2004, RS 152.3
N	note(s) marginale(s)
NAVS13	numéro AVS à 13 chiffres
no	numéro(s)
not.	notamment
NSA	National Security Agency
OAMal	Ordonnance sur l'assurance-maladie du 27 juin 1995, RS 832.102
OBI	Organisation de l'infrastructure ferroviaire
OCPD	Ordonnance sur les certifications en matière de protection des données du 28 septembre 2007, RS 235.13
OFJ	Office fédéral de la justice
OFPER	Office fédéral du personnel
OFSP	Office fédéral de la santé publique
OHand	Ordonnance sur l'élimination des inégalités frappant les personnes handicapées (Ordonnance sur l'égalité pour les handicapés) du 19 novembre 2003, RS 151.31
OLAA	Ordonnance sur l'assurance-accidents du 20 décembre 1982, RS 832.202
OLPD	Ordonnance relative à la loi fédérale sur la protection des données du 14 juin 1993, RS 235.11
OLT3	Ordonnance 3 relative à la loi sur le travail du 18 août 1993, RS 822.133

OPAS	Ordonnance du DFI sur les prestations dans l'assurance obligatoire des soins en cas de maladie (Ordonnance sur les prestations de l'assurance des soins) du 29 septembre 1995, RS 832.112.31
OPDC	Ordonnance concernant la protection des données personnelles du personnel de la Confédération du 26 octobre 2011, RS 172.220.111.4
OPers	Ordonnance sur le personnel de la Confédération du 3 juillet 2001, RS 172.220.111.3
OPrl	Ordonnance concernant la protection des informations de la Confédération (Ordonnance concernant la protection des informations) du 4 juillet 2007, RS 510.411
OR	Bundesgesetz betreffend die Ergänzung des Schweizerischen Zivilgesetzbuches (Fünfter Teil: Obligationenrecht) vom 30. März 1911, SR 220
ORAb	Ordonnance contre les rémunérations abusives dans les sociétés anonymes cotées en bourse du 20 novembre 2013, RS 221.331
OSE	Ordonnance sur le service de l'emploi et la location de services du 16 janvier 1991, RS 823.111
OTrans	Ordonnance sur le principe de la transparence dans l'administration (Ordonnance sur la transparence) du 24 mai 2006, RS 152.31
p./pp.	page/pages
PA	Loi fédérale sur la procédure administrative du 20 décembre 1968, RS 172.021
par.	paragraphe(s)
PFPDT	Préposé fédéral à la protection des données et à la transparence
PJA	Pratique juridique actuelle
RAI	Règlement sur l'assurance-invalidité du 17 janvier 1961, RS 831.201
RDAF	Revue de droit administratif et de droit fiscal
REAS	Responsabilité et Assurances (revue)
réf.	référence(s)
RéLIPDA	Règlement d'exécution de la loi vaudoise sur l'information du public, la protection des données et l'archivage du 16 décembre 2010, RSV 170.200
resp.	respectivement
RFJ	Revue fribourgeoise de jurisprudence
RGPD	Règlement (UE) 2016/679 du Parlement européen et du Conseil relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données) du 27 avril 2016
RIPOL	Système de recherches informatisées de police
RJB	Revue de la Société des juristes bernois
RJJ	Revue jurassienne de jurisprudence
RJN	Recueil de jurisprudence neuchâteloise
RS	Recueil systématique des lois fédérales (ou cantonales)

RSAS	Revue suisse des assurances sociales et de la prévoyance professionnelle
RSDA	Revue suisse de droit des affaires et du marché financier
RSJ	Revue suisse de jurisprudence
RSPC	Revue suisse de procédure civile
RSt	Règlement général neuchâtelois d'application de la loi sur le statut de la fonction publique du 9 mars 2005, RSN 152.511
RTFP	Règlement neuchâtelois concernant les traitements de la fonction publique du 9 mars 2005, RSN 152.511.10
RVJ	Revue valaisanne de jurisprudence
s/ss	suivant/suivants
SECO	Secrétariat d'Etat à l'économie
SEV	Syndicat du personnel des transports
sic !	Revue du droit de la propriété intellectuelle, de l'information et de la concurrence
SJ	Semaine Judiciaire
SMR	Service médical régional
SOR	Second Œuvre Romand
SSPP	Société suisse de psychiatrie et psychothérapie
supra	plus haut
SUVA	Schweizerische Unfallversicherungsanstalt (CNA, Caisse nationale suisse d'assurance en cas d'accidents)
TAF	Tribunal administratif fédéral
TF	Tribunal fédéral
TFA	Tribunal fédéral des assurances
TPI	Tribunal de première instance
trad.	traduction
UE	Union européenne
UPIC	Unité de pilotage informatique de la Confédération
USIC	Unité de stratégie informatique de la Confédération
VwVG	Bundesgesetz über das Verwaltungsverfahren (Verwaltungsverfahrensgesetz) vom 20. Dezember 1968, SR 172.021
ZBJV	Zeitschrift des bernischen Juristenvereins
ZBl	Schweizerisches Zentralblatt für Staats- und Verwaltungsrecht
ZPO	Schweizerische Zivilprozessordnung vom 19. Dezember 2008, SR 272

PREMIERE PARTIE

Principes généraux

CHRISTIAN FLUECKIGER*

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

Sommaire Page

I. Introduction 2

II. Nouveautés législatives à venir 2

III. Marche à suivre pour vérifier la licéité d'un traitement de données personnelles 3
A. Commune à tous les traitements 4
1. Règles applicables 4
a) Détermination de l'application du droit cantonal ou fédéral 4
b) Exceptions au champ d'application 6
2. Données traitées 6
3. Présence d'un motif justificatif 7
a) Base légale 8
b) Consentement 9
c) Intérêt prépondérant public/privé 10
4. Respect des principes généraux 10
a) La légalité 10
b) La bonne foi 11
c) La proportionnalité 11
d) La finalité 12
e) La reconnaissabilité 13
f) L'exactitude 14
g) La sécurité des données 14
B. Propre aux communications transfrontières de données personnelles 15
a) Niveau de protection adéquat 15
b) Communications dans un pays possédant une législation adéquate 17
c) Communications dans un pays ne possédant pas une législation adéquate 18
C. Propre à la sous-traitance 21

IV. Conclusions 21

Bibliographie 22

* Je remercie Mme Valérie Gigon pour ses précieuses, efficaces et indispensables relectures.

I. Introduction

Les principes généraux de la protection des données figurant dans le droit européen, fédéral et cantonal ont déjà fait couler beaucoup d'encre depuis le début des années nonante. Afin d'offrir, tant que faire se peut, des nouveautés aux lecteurs, cette contribution propose un examen des principes généraux ciblé sur les traitements de données dans le cadre des relations de travail, mais surtout suggère une approche pragmatique pour l'analyse des cas d'espèce. Elle a l'espoir, trop ambitieux peut-être au vu des contraintes inhérentes à ce type de publication, d'essayer de faciliter la tâche des responsables d'entreprises confrontés à la problématique de l'analyse de la conformité des traitements de données relatifs à leurs collaborateurs, sans forcément être des juristes aguerris dans ce domaine.

Suite à la victoire de l'autrichien Max Schrems devant la Cour de justice de l'Union européenne (CJUE) face à Facebook[1], les communications de données personnelles transfrontières sont source de vives inquiétudes pour les entreprises. C'est pourquoi ce thème sera également abordé, afin de tenter d'apporter des débuts de réponses au regard de l'évolution des règles de la protection des données.

II. Nouveautés législatives à venir

Le Parlement de l'Union européenne a adopté le 27 avril 2016 une nouvelle directive relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel[2]. Celle-ci faisant partie de l'acquis Schengen, les autorités suisses ont décidé d'étendre son application à l'ensemble des traitements de données et non pas exclusivement au domaine pénal[3]. Parallèlement, le Conseil de l'Europe a élaboré un projet de révision[4] de la Convention STE 108[5]. Pour respecter leurs obligations vis-à-vis

1 Arrêt CJUE C-362/14 Maximillian Schrems c. Data Protection Commissioner du 6 octobre 2015.

2 Directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil (JO L 119 du 4 mai 2016, p. 89).

3 Rapport explicatif du 21 décembre 2016 concernant l'avant-projet de loi fédérale sur la révision totale de la loi sur la protection des données et sur la modification d'autres lois fédérales, pp. 27 s.

4 http://www.coe.int/fr/web/data-protection/modernisation-convention108.

5 Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, RS 0.235.1.

du droit international, les autorités suisses ont lancé des processus de révision de leurs règles sur la protection des données. Le Conseil fédéral a mis en consultation un projet de révision[6] de la LPD[7].

Ce dernier et les révisions des lois cantonales de protection des données ne devraient pas entrer en vigueur avant le deuxième semestre 2018, dans le meilleur des cas. D'ici là, les explications qui suivent resteront pleinement d'actualité. Ensuite, elles resteront a priori toujours applicables, sous réserve de quelques menus détails, surtout au niveau des références légales.

III. Marche à suivre pour vérifier la licéité d'un traitement de données personnelles

Dans le cadre de la protection des données personnelles, la notion de traitement comprend toute opération relative à des données personnelles, quels que soient les moyens et procédés utilisés, notamment la collecte, la conservation, l'exploitation, la modification, la communication, l'archivage ou la destruction de données[8]. Bien que ces opérations soient incontournables dans toutes les entreprises, il n'est pas toujours facile de déterminer si elles s'effectuent dans la légalité ou non, alors que les règles fédérales de la protection des données sont en vigueur depuis 1993.

Cette relative difficulté provient peut-être du fait que cette matière relève parallèlement du droit cantonal et fédéral, et qu'elle fasse l'objet de lois contenant les principes généraux ainsi qu'un nombre considérable de lex specialis disséminées dans le vaste ensemble de règles de droit cantonal et fédéral[9]. Mettre la main sur ces dernières n'est pas toujours aisé, de même que l'articulation avec les principes généraux, sans compter la détermination du droit applicable lorsque le traitement est susceptible de toucher le droit cantonal et fédéral.

C'est pourquoi cette contribution propose une marche à suivre destinée à faciliter l'examen de la licéité des traitements de données. Au premier regard, notamment sur le nombre de sous-titres ci-après, cette démarche peut sembler ardue et complexe. Après un petit peu de pratique, des automatismes naissent rapidement et la rendent beaucoup plus digeste.

---

6 Rapport explicatif du 21 décembre 2016 concernant l'avant-projet de loi fédérale sur la révision totale de la loi sur la protection des données et sur la modification d'autres lois fédérales.

7 Loi fédérale sur la protection des données (LPD), RS 235.1.

8 Art. 3 let. e LPD.

9 Pour s'en convaincre, il suffit de faire dérouler la rubrique 235, Protection des données, figurant sur cette page : https://www.admin.ch/opc/fr/classified-compilation/23.html.

Rappelons néanmoins que cette marche à suivre proposée ici n'est destinée qu'au cadre restreint des relations de travail. Même si l'éclairage portera en premier lieu sur le droit privé fédéral, les principales différences avec les droits cantonaux seront également évoquées.

A. Commune à tous les traitements

Les dix examens développés ci-après s'imposent à tous les traitements de données personnelles, quels qu'ils soient. Mais selon le résultat de la vérification, la démarche peut s'interrompre en cours de route et ainsi être facilitée.

1. Règles applicables

a) Détermination de l'application du droit cantonal ou fédéral

Dans l'esprit de beaucoup, la distinction entre les règles fédérales et cantonales de protection des données n'est absolument pas claire. Les préposés cantonaux à la protection des données sont régulièrement sollicités pour des sujets fédéraux et inversement. Ils sont souvent considérés comme des « antennes » du préposé fédéral à la protection des données et à la transparence (PFPDT) pour les traitements effectués dans les cantons.

Or, le droit applicable dépend avant tout des caractéristiques du responsable du traitement de données personnelles et en second lieu du territoire. Plus concrètement, les organes fédéraux sont soumis à la LPD, alors que les cantonaux, ainsi que les communaux, sont soumis au droit cantonal. Les entreprises privées (personnes physiques et morales relevant du droit privé) sont en principe soumises à la LPD. Mais si elles effectuent une tâche d'intérêt public, elles sont soumises au droit de l'entité pour le compte de laquelle elles l'accomplissent.

Même si parfois la notion d'organe fédéral, voire cantonal/communal, est discutée devant les tribunaux[10], c'est surtout la question de savoir si une entreprise privée effectue une tâche d'intérêt public soumise au droit cantonal qui effraie le plus souvent.

Selon une ancienne jurisprudence neuchâteloise, seules « *les tâches dont le législateur considère que l'État doit se charger en lieu et place de particuliers* »[11], doivent être qualifiées d'intérêt public. Une analyse doctrinale de la jurisprudence permet de préciser et développer les critères facilitant la qualification. La notion de tâche publique signifie

[10] TF 1C_125/2015 du 17 juillet 2015, c. 2 ; TAF A-971/2015 du 16 juin 2016 ; ATAF 2015/43, c. 6.2 ss, p. 627 (631 ss).

[11] RJN 1987, p. 124, c. 2c.

que l'employeur privé (quelle que soit la forme juridique[12]) doit être obligé par la Constitution, une loi ou par délégation (mandat de prestation), à effectuer durablement une activité, et non pas se limiter à tolérer ou s'abstenir. Aucune tâche publique n'est déléguée lorsque l'administration se procure les moyens nécessaires pour accomplir ses tâches publiques auprès de personnes privées[13]. Par exemple, des entreprises construisant une école, livrant des fournitures de bureau ou du matériel n'accomplissent pas une tâche publique. Les critères suivants ne sont pas relevants pour établir qu'il s'agit d'une tâche publique : forme de l'organisation, forme des prestations, régime en matière de responsabilité, obligation de tenir compte des droits fondamentaux, octroi de subventions[14], pilotage de l'État, surveillance de l'État[15], initiative étatique ou privée, concurrence, subsidiarité de l'accomplissement de la tâche, ou concession[16]. De plus, une entreprise en main exclusive de collectivités publiques n'accomplit pas forcément une tâche d'intérêt public[17].

Malgré l'existence de ces précisions, il n'est pas toujours facile de déterminer si la tâche examinée est attribuable directement ou indirectement à une entreprise privée. Par exemple, en matière de transport, cette activité n'est pas à la charge des autorités neuchâteloises, car la loi ne leur attribue que la charge d'octroyer ou non une concession à des entreprises de transport[18]. En revanche, la loi impose à celles-ci d'assurer la sécurité des passagers[19]. Par conséquent, la compagnie de transport neuchâteloise TransN est soumise à la LPD pour le traitement des données de ses employés, mais à la CPDT-JUNE[20] pour les traitements relatifs aux contrôles des titres de transport. On retrouve ce genre de problématique avec les entreprises d'électricité[21], les hôpitaux privés[22] et encore bien d'autres acteurs.

Quoi qu'il en soit, les principes généraux à respecter étant les mêmes dans les droits cantonaux que dans le droit fédéral, l'impact de la distinction concerne surtout les modalités de justification du traitement de données, la détermination du préposé compétent pour la surveillance et quelques obligations à respecter (déclaration du fichier,

12 RJN 1991, p. 84, c. 2b ; RJN 1999, p. 182, c. 2b.
13 RÜTSCHE, Surveillance, pp. 71 ss.
14 RJN 1999, p. 182, c. 2a.
15 CDP.2014.172 du 9 juin 2015.
16 RÜTSCHE, p. 162 ; RÜTSCHE, Surveillance, p. 77 ; arrêt de la Cour de droit public neuchâteloise CDP.2014.172 du 9 juin 2015.
17 RJN 1991, p. 84, c. 3a et 3b ; 1987, p. 124 ; 1983, p. 124.
18 Art. 11 Loi cantonale sur les transports publics (LTP, RSN 765.1).
19 Art. 2 Loi fédérale sur les organes de sécurité des entreprises de transports publics (LOST, RS 745.2).
20 Convention intercantonale relative à la protection des données et à la transparence dans les cantons du Jura et de Neuchâtel, RSN 150.30.
21 ATF 131 II 1 (5), c. 3.2.
22 RÜTSCHE, Surveillance, p. 69.

certification, modalités de sous-traitance, étendue du devoir d'information, nécessité d'une base légale,…).

b) Exceptions au champ d'application

Avant de passer au point suivant, il ne faut pas oublier de vérifier si le traitement en cause n'entre pas dans l'une des exceptions du champ d'application du droit applicable. Pour sa part, la LPD exclut les données personnelles qu'une personne physique traite pour un usage exclusivement personnel et qu'elle ne communique pas à des tiers, les données personnelles traitées par le Comité international de la Croix-Rouge, les registres publics relatifs aux rapports juridiques de droit privé, ainsi que les délibérations des Chambres fédérales et des commissions parlementaires. Il en va de même pour les procédures pendantes civiles, pénales, d'entraide judiciaire internationale ainsi que de droit public et de droit administratif, à l'exception des procédures administratives de première instance[23]. Les droits cantonaux connaissent tous des exceptions relatives aux procédures pendantes, voire également aux activités soumises à une concurrence économique.

2. Données traitées

Il ne faut jamais perdre de vue que les règles de la protection des données ne s'appliquent qu'aux données personnelles. C'est-à-dire toutes les informations qui se rapportent à une personne identifiée ou identifiable[24]. Tel est le cas lorsque, « *par corrélation indirecte d'informations tirées des circonstances ou du contexte, on peut identifier une personne (p. ex. lorsque, à partir de données concernant des biens immobiliers, on peut remonter au propriétaire)* »[25]. Par exemple, le Tribunal fédéral a eu l'occasion de préciser, dans le fameux arrêt Logistep, que les adresses IP étaient des données personnelles[26], de même que les images et les sons de personnes. Les données qualifiées de sensibles sont particulièrement protégées, telles que celles relatives aux opinions ou activités religieuses, philosophiques, politiques ou syndicales, à la santé, à la sphère intime ou à l'appartenance à une race, aux mesures d'aide sociale, aux poursuites ou sanctions pénales et administratives[27]. S'ajouteront certainement à cette liste les données génétiques et biométriques identifiant un individu de façon unique lorsque la LPD sera révisée[28].

---

23 Art. 2 al. 2 LPD.

24 Art. 3 let. a LPD.

25 FF 1988 II 421 (452).

26 ATF 136 II 508.

27 Art. 3 let. c LPD.

28 Rapport explicatif du 21 décembre 2016 concernant l'avant-projet de loi fédérale sur la révision totale de la loi sur la protection des données et sur la modification d'autres lois fédérales, p. 42.

A contrario, les données statistiques ou anonymisées ne sont pas soumises aux exigences des règles de la protection des données. Mais il ne faut pas oublier qu'une anonymisation doit empêcher, de façon irréversible, toute identification[29], faute de quoi il s'agit d'une pseudonymisation, qui reste soumise à celles-ci. Par exemple, un tableau Excel dans lequel figurent uniquement les salaires et le nombre d'enfants des employés pourrait être considéré comme contenant des données personnelles dans une petite entreprise.

3. Présence d'un motif justificatif

La logique voudrait qu'il soit d'abord vérifié si le traitement cause une atteinte illicite à la personnalité, avant d'examiner si cette dernière est justifiée. Mais pour des raisons d'efficacité, il est plus judicieux d'effectuer la démarche dans l'ordre inverse[30].

Un traitement de données personnelles (*supra* III.A.1) soumis au droit fédéral (*supra* III.A.2) peut être justifié de trois manières différentes, la loi, le consentement ou l'intérêt prépondérant public ou privé. Il suffit que l'entreprise privée puisse se prévaloir de l'un de ces trois motifs pour que le traitement respecte les exigences de la protection des données, pour autant que les principes généraux ne soient violés qu'avec retenue[31]. À l'heure actuelle, il faut encore, par acquit de conscience, vérifier que cette dernière condition soit respectée. Cependant, il est très probable que la révision de la LPD, et plus particulièrement la reformulation de l'article 12 LPD, facilitera la démarche en permettant d'éviter ce contrôle[32].

En l'absence d'un motif justificatif, il reste donc à déterminer si le traitement de données personnelles examiné cause ou non une atteinte illicite à la personnalité. Pour ce faire, il faut examiner si tous les principes généraux sont respectés (*infra* III.A.4).

Au niveau cantonal, seuls les deux premiers motifs entrent en ligne de compte, puisque tout acte étatique doit se fonder sur une base légale[33], y compris les traitements de données. Or, lors de l'adoption d'une base légale, il est effectué l'examen de l'intérêt public/privé prépondérant.

---

29 Groupe de travail « Article 29 », p. 3.

30 Pour plus de détails, voir FLUECKIGER, Googlelisation, pp. 89 ss.

31 ATF 136 II 508, c. 5.2.4, *in* : JdT 2011 II 446.

32 Rapport explicatif du 21 décembre 2016 concernant l'avant-projet de loi fédérale sur la révision totale de la loi sur la protection des données et sur la modification d'autres lois fédérales, p. 65.

33 Zen-Ruffinen, p. 35.

a) Base légale

En droit privé, l'article 328b CO[34] constitue l'une des principales bases légales justifiant de traiter des données personnelles d'employés. Il offre la présomption que les traitements de données personnelles portant sur les aptitudes de l'employé à remplir son emploi ou nécessaires à l'exécution du contrat de travail sont licites[35].

Concrètement, l'employeur peut obtenir ou conserver temporairement, des références d'anciens employeurs, tests, cursus scolaire et professionnel, diplômes et certificats de travail, connaissances linguistiques, autorisations d'exercer (professions réglementées), état civil, date de naissance, nationalité, numéro AVS, domicile, enfants, références bancaires, données relatives au salaire et aux assurances, renseignements relatifs aux arrêts de travail et aux vacances, évaluations, cours de perfectionnement, mesures disciplinaires, correspondances avec l'employé ou encore plan de carrière[36]. L'étendue des données personnelles pouvant être traitées doit plutôt être restrictive, surtout lorsqu'elles concernent de près ou de loin la santé de l'employé[37]. Conformément à ce que semblent affirmer la jurisprudence et la doctrine majoritaire, cette disposition s'applique également dans la phase d'engagement des employés, c'est-à-dire avant la conclusion du contrat de travail[38].

D'autres dispositions légitiment également des traitements de données par les employeurs. Par exemple, l'article 6 LTr[39] permet les traitements de données destinés à atteindre le but de protection de la santé ; l'article 22 LAGH[40] autorise à certaines conditions qu'un médecin effectue une analyse génétique présymptomatique sur un employé ; les articles 18 al. 3 LSE[41] et 47 OSE[42] permettent à un bailleur de service de traiter les données nécessaires au placement d'un demandeur d'emploi ; l'article 957 CO impose aux employeurs de tenir une comptabilité, comprenant évidemment les données salariales des employés ; l'article 45 LHID[43] oblige les employeurs à fournir une attestation fiscale sur

34 Code des obligations, RS 220.
35 ATF 130 II 425 (434), c. 3.3.
36 DUNAND, N 27 et 29 *ad* art. 328b CO, p. 326 et références citées, ainsi que N 41 ss, p. 328 ; PFDPT, Guide, p. 12.
37 Pour plus de détails, voir FLUECKIGER, N 320 ss, pp. 98 ss.
38 AUBERT, p. 156 ; GRAND, p. 52 ; FLUECKIGER, N 315 ss, pp. 97 s et références citées ; ATF 122 V 267 ; pour un avis contraire, MANAÏ, p. 145.
39 Loi fédérale sur le travail dans l'industrie, l'artisanat et le commerce, RS 822.11.
40 Loi fédérale sur l'analyse génétique humaine, RS 810.12.
41 Loi fédérale sur le service de l'emploi et la location de services, RS 823.11.
42 Ordonnance sur le service de l'emploi et la location de services, RS 823.111.
43 Loi fédérale sur l'harmonisation des impôts directs des cantons et des communes, RS 642.14.

les avantages reçus par les collaborateurs ; l'article 7 LDét[44] oblige les employeurs à remettre aux organes de contrôle tous les documents attestant que les conditions de travail et de salaire des travailleurs sont respectées[45] ; les articles 50a LAVS[46], ainsi que 66 et 66a LAI[47] permettent aux employeurs de communiquer des données à un certain nombre d'acteurs en matière d'AVS/AI.

En droit public cantonal, les lois sur le personnel constituent les principales bases légales, mais des dispositions pertinentes peuvent également être disséminées dans d'autres bases légales, telles que les règlements spécifiques à certaines professions.

b) Consentement

Une personne concernée par un traitement de données personnelles ne consent valablement que si elle exprime sa volonté librement et après avoir été dûment informée. Lorsqu'il s'agit de données sensibles et de profils de la personnalité, son consentement doit être au surplus explicite[48]. Dans le cadre des relations de travail, l'examen de la condition de la liberté ne doit pas être effectué à la légère. À la lecture du message du Conseil fédéral, il ressort que le consentement de l'employé est libre si l'employeur indique à ce dernier les conséquences d'un refus, pour autant qu'elles ne soient pas disproportionnées par rapport au but du traitement, comme par exemple la menace d'un licenciement ou un traitement de données qui n'est pas nécessaire à l'exécution du contrat de travail[49]. Conformément à l'article 362 CO, il n'est pas possible d'effectuer un traitement de données sortant du cadre imposé par l'article 328b CO (*supra* III.A.3.a) au détriment de l'employé, même avec le consentement de ce dernier[50]. Le consentement n'est soumis à aucune forme dans le cadre des relations de travail. Mais il est toujours plus prudent de conserver une trace écrite en cas de litige.

Les exigences pour l'obtention d'un consentement valable sont similaires en droit public cantonal.

---

44 Loi fédérale sur les mesures d'accompagnement applicables aux travailleurs détachés et aux contrôles des salaires minimaux prévus par les contrats-types de travail, RS 823.20.

45 TF 2C_625/2016 du 12 décembre 2016.

46 Loi fédérale sur l'assurance-vieillesse et survivants, RS 831.10.

47 Loi fédérale sur l'assurance-invalidité, RS 831.20.

48 Art. 4 al. 5 LPD.

49 FF 2003 1915 (1939 s) ; ATAF 2009/44, c. 4.1, p. 620 (631) ; JdT 2010 I 396 (405).

50 DUNAND, N 32 *ad* art. 328b CO, p. 327 ; dans le même sens, MEIER, N 2026, p. 647 et N 2107 ss, pp. 677 ss.

c) Intérêt prépondérant public/privé

La détermination de la prépondérance d'un intérêt privé/public sur un autre est une affaire d'appréciation qui est toujours très délicate à trancher. D'autant plus qu'elle doit s'effectuer au cas par cas et que la jurisprudence n'est pas légion en la matière. La doctrine donne quelques exemples, notamment en matière de sauvegarde de l'intégralité des e-mails entrants et sortants de la messagerie professionnelle, d'utilisation de photographies publicitaires, de récolte du numéro de téléphone mobile, de dénonciation pénale[51], mais qui sont largement insuffisants pour pouvoir juger si les conditions de la justification sont remplies. L'énumération des exemples d'intérêts publics et privés prépondérants figurant à l'article 13 al. 2 LPD n'est pas d'un plus grand secours, l'étendue de l'application de chacun étant soumise à interprétation.

4. Respect des principes généraux

S'il n'a pas été possible de justifier le traitement de données personnelles des employés à l'aide de l'un des trois motifs ci-avant, il reste donc à vérifier si les principes généraux de la protection des données sont tous respectés, sans exception. Le cas échéant, le traitement de données personnelles examiné pourra alors être déclaré conforme aux exigences des règles de la protection des données.

a) La légalité

Les employeurs ne sont pas en droit de traiter des données s'ils enfreignent une disposition légale protégeant directement ou indirectement la personnalité des employés[52]. Il n'est notamment pas autorisé de réaliser un traitement en violant les articles 28 et 29 CO[53], 143, 143bis, 146,147, 179, 179bis, 179ter, 179^{quater}, 181, 186, 320 ou 321 CP[54], ainsi que 47 LB[55], 26 OLT3[56] et 328 CO.

---

51 MEIER, N 2039, pp. 651 s et les références citées ; DUNAND, N 30 s *ad* art. 328b CO, p. 327 et les références citées.

52 MEIER, N 640, p. 261.

53 Code des obligations, RS 220.

54 Code pénal, RS 311.0.

55 Loi fédérale sur les banques et les caisses d'épargne, RS 952.0 ; MEIER, N 641, p. 262 ; FLUECKIGER, N 201, p. 61.

56 Ordonnance relative à la loi sur le travail, RS 822.113.

b) La bonne foi

En reprenant l'inévitable principe de l'article 2 CC[57], le législateur a voulu insister et renforcer son respect dans le cadre du traitement des données. Les employeurs ne sont ainsi pas en droit de traiter des données à l'insu ou contre la volonté des employés. Ils sont au contraire dans l'obligation de mentionner l'existence du traitement qui doit être reconnaissable, mais également l'utilisation qui sera faite des données[58]. Par exemple, une entreprise viole ce principe si elle ne détruit pas des dossiers de candidature, alors qu'elle s'y était engagée[59], ou qu'elle transmet des données d'un employé à des tiers sans qu'il s'y attende[60].

c) La proportionnalité

De manière générale, le Tribunal fédéral a déjà eu maintes fois l'occasion de définir ce principe[61]. Dans le cadre spécifique de la protection des données, le principe de la proportionnalité exige qu'un traitement de données soit apte à atteindre les buts fixés (règle de l'aptitude) et que ceux-ci ne puissent être atteints par un traitement ou une démarche le moins intrusifs possible dans la vie privée (règle de la nécessité) ; en outre, il interdit tout traitement allant au-delà du but visé et il exige un rapport raisonnable entre celui-ci et la protection de la personnalité des personnes concernées (principe de la proportionnalité au sens étroit, impliquant une pesée des intérêts)[62]. Bien qu'à la lecture de l'article 328b CO, on soit tenté de croire que cette disposition est une concrétisation de ce principe en droit privé[63], il faut plutôt désormais considérer cette disposition comme une présomption légale que les données qui lui sont soumises ne portent pas atteinte à la personnalité du travailleur[64], même si cela fait l'objet d'un conflit doctrinal[65].

Quoi qu'il en soit, cela signifie par exemple qu'un employeur doit effacer les données de ses employés sitôt qu'elles ne sont plus nécessaires, ne pas les « ficher » comme l'avait fait Orange[66], ne pas effectuer des assessments ou autres tests trop intrusifs dans la sphère privée, voire intime[67], ne pas récolter, sauf exception, des données relatives à la

---

57 Code civil, RS 210.
58 FLUECKIGER, N 204, p. 62.
59 MEIER, N 655, p. 266.
60 TAF A-5326/2015 du 26 août 2016, c. 4.4.4.
61 TF 8C_702/2015 du 15 juin 2016, c. 6.4.3 et références citées.
62 TF 8C_702/2015 du 15 juin 2016, c. 6.4.1 s.
63 DUNAND, N 4 *ad art.* 328b CO, p. 319 ; FLUECKIGER, N 210, p. 64.
64 DUNAND, N 4 *ad* art. 328b CO, p. 319.
65 DU PASQUIER/OBERSON/FISCHER, pp. 30 s.
66 Employés fichés, Orange se défend, *in* : L'Impartial, 17 juin 2003, p. 27.
67 PFPDT, Guide, p. 9.

séropositivité, à la volonté d'avoir des enfants, au cercle d'amis, fréquentations, tendances sexuelles, à la situation financière, aux opinions du candidat[68], ne pas « googleliser » ses employés pour enquêter sur leur vie privée[69], ainsi que s'assurer que les accès des collaborateurs soient limités aux seules données indispensables pour accomplir leurs tâches. En revanche l'employeur est en droit de savoir si un employé est syndiqué lorsque cela permet de déterminer s'il est soumis ou non à une CCT et que cela influence le montant du salaire[70] ; de mandater un médecin pour effectuer des tests de dépistage de drogue pour des raisons de sécurité[71]. De manière générale, les traitements de données effectués dans le cadre des dossiers de candidature, d'entretiens d'embauche, tests de recrutement, de recherches sur internet, de l'état de santé, de la gestion du dossier de l'employé ou la surveillance des employés, ne peuvent se faire que sous réserve du respect d'un certain nombre de modalités[72]. Selon le Conseil fédéral, les employeurs ne peuvent qu'exceptionnellement invoquer l'article 12 al. 3 LPD, c'est-à-dire qu'il n'y a pas atteinte à la personnalité lorsque la personne concernée a rendu les données accessibles à tout un chacun et ne s'est pas opposée formellement au traitement, lorsqu'ils récoltent des données à propos de leurs employés sur internet[73].

d) La finalité

Les données des employés ne doivent être traitées que dans le but indiqué lors de leur collecte, prévu par une loi ou qui ressort des circonstances[74]. Dans le cadre des relations de travail soumises au droit privé, l'article 328b CO n'autorise les traitements de données des employés que pour évaluer leur aptitude ou l'exécution du contrat de travail. Toute autre finalité conduirait inévitablement à un traitement de données illicite. Même si le Tribunal fédéral n'a pas lié ses considérations avec une violation du principe de la finalité, il est néanmoins intéressant de retenir qu'un employé a été licencié avec effet immédiat parce qu'il avait récolté des données au sujet d'une collègue sans raison valable[75].

Les employeurs soumis au droit cantonal de la protection des données ne peuvent traiter les données des employés que dans un des buts figurant dans une base légale.

---

68 DUNAND, N 28 *ad* art. 328b CO, p. 326 et N 46 s *ad* art. 328b CO, pp. 330 s.

69 WILDHABER/HÄNSENBERGER, p. 326 ; DUNAND, N 59 *ad* art. 328b CO, p. 335 ; FLUECKIGER, Googlelisation, pp. 92 s.

70 ATF 123 III 129 (134), c. 3b, cc.

71 PFPDT, Guide, p. 10.

72 DUNAND, N 41 ss *ad* art. 328b CO, pp. 329 ss et références citées.

73 Pour plus de détail voir CONSEIL FÉDÉRAL, p. 58 et références citées.

74 Art. 4 al. 3 LPD.

75 TF 8C_62/2014 du 29 novembre 2014, c. 2.3.2.

e) La reconnaissabilité

L'employeur, privé ou public, a l'obligation d'informer les employés de toute collecte de données sensibles ou de profils de la personnalité les concernant, que la collecte soit effectuée directement auprès d'eux ou auprès d'un tiers. Il doit notamment leur indiquer l'identité du maître de fichier, la finalité du traitement pour lequel les données sont collectées et les catégories de destinataires des données, en cas de communication de ces dernières. Si les données ne sont pas collectées auprès de la personne concernée, elle doit en être informée au plus tard lors de leur enregistrement ou, en l'absence d'un enregistrement, lors de la première communication à un tiers[76]. Bien que la LPD prévoie des exceptions à ce devoir d'information, il est peu probable qu'elles puissent se réaliser dans le cadre d'une relation de travail[77]. Jusqu'à présent, au vu des rares données sensibles[78] que l'employeur était susceptible d'être en droit de traiter, le devoir d'information pouvait être respecté sans même que les parties en soient conscientes. Par exemple, lorsqu'une banque demandait un extrait du casier judiciaire, les conditions précitées étaient usuellement respectées, sans forcément concevoir que la LPD imposât la communication des détails énumérés ci-dessus.

Cependant, il est fort probable que ces exigences s'appliqueront à l'ensemble des données lors de l'entrée en vigueur de la révision en cours de la LPD (*supra* II)[79]. Cette nouveauté exigera beaucoup d'effort de la part des employeurs qui devront systématiquement accomplir leur devoir d'information et surtout pouvoir justifier qu'ils l'ont rempli. Or, toute attestation de justification entraînera des tâches administratives et la mise sur pied de processus d'autocontrôles supplémentaires.

À noter qu'actuellement déjà, les employeurs ne peuvent posséder un dossier caché (dossier gris) parallèle au dossier officiel[80] ou contrôler l'utilisation du réseau internet professionnel par les employés qu'en respectant strictement certaines modalités[81]. Ils ne sont également pas en droit d'installer un GPS sur un véhicule à l'insu d'un employé[82].

---

76 Art. 14 LPD.

77 Art. 14 al. 4 LPD.

78 Les données sont les données personnelles relatives aux opinions ou activités religieuses, philosophiques, politiques ou syndicales ; à la santé, la sphère intime ou l'appartenance à une race ; aux mesures d'aide sociale, aux poursuites ou sanctions pénales et administratives (art. 3 let. c LPD).

79 Rapport explicatif du 21 décembre 2016 concernant l'avant-projet de loi fédérale sur la révision totale de la loi sur la protection des données et sur la modification d'autres lois fédérales, p. 38.

80 DUNAND, N 77 *ad* art. 328b CO, p. 340.

81 JAR 2015 666 (668) ; arrêt de la Cour jurassienne administrative ADM 92/2009 du 25 février 2013 ; RJJ 2013 p. 87 ; DUNAND N 85 ss *ad* art. 328b CO, pp. 342 s.

82 Arrêt de la Chambre d'accusation neuchâteloise CHAC.2010.23 du 14 juin 2010.

f) L'exactitude

Les employeurs privés ou publics doivent s'assurer que les données traitées relatives aux employés sont correctes. Ils doivent prendre toute mesure appropriée permettant d'effacer ou de rectifier les données inexactes ou incomplètes au regard des finalités pour lesquelles elles ont été collectées ou sont traitées. Les employés concernés peuvent requérir la rectification de leurs données inexactes[83]. Selon le PFPDT, « *Il existe différents types de données inexactes. Il y a des données totalement incorrectes (p. ex: nom mal orthographié, fausse date de naissance) et des données qui sont en soi exactes mais qui, réunies, donnent une vision partielle, voire fausse, de la réalité. La question de savoir dans quelle mesure l'exactitude relative de données personnelles doit, dans une situation précise, être assimilée à des données inexactes au sens de la LPD ne peut être tranchée qu'en considérant la finalité et la manière de traiter les données*. »[84]. Concrètement, un employeur peut traiter l'information qu'un employé sent l'alcool tous les matins depuis un an, mais ne peut pas le qualifier d'alcoolique. Il peut aussi retenir qu'un employé commet régulièrement de nombreuses fautes dans les courriers qu'il rédige, mais pas qu'il est nul en orthographe. De même, que l'employé a un comportement menaçant envers un collègue, mais pas qu'il a un comportement sanguin au vu de son origine.

Par ailleurs, la justice neuchâteloise a eu l'occasion d'affirmer qu'il n'était pas sérieux de traiter l'information qu'un collaborateur souffrait d'un trouble de la vision incompatible avec les exigences de sa fonction, information fondée sur une conversation improbable entre l'employeur et un psychiatre, alors que l'acuité et le champ visuels du collaborateur avaient été considérés comme normaux par un ophtalmologue[85]. Le Tribunal fédéral a quant à lui confirmé la condamnation d'un employeur pour avoir donné des renseignements faux et manifestement dépréciatifs à un potentiel nouvel employeur[86]. En revanche, il est possible de conserver l'inscription d'un soupçon d'abus dans le dossier d'un employé, même s'il s'est avéré totalement infondé, ce résultat doit alors également y figurer afin d'éviter toute fausse interprétation, à laquelle conduirait fatalement une information incomplète[87].

g) La sécurité des données

Les employeurs, privés ou publics, se doivent d'assurer la sécurité technique des données personnelles qu'ils traitent, conformément à l'article 7 LPD. Ils doivent éviter tout traitement non autorisé par des mesures organisationnelles et techniques appropriées.

---

83 Art. 5 LPD.

84 PFPDT, Rapport, p. 307.

85 Arrêt de la Cour de droit public neuchâteloise CDP.2010.443 du 20 juillet 2011.

86 TF 4A_117/2013 du 31 juillet 2013, c. 2.2.

87 TF 1A_6/2001 du 2 mai 2001, c. 2.1.

Autrement dit, l'employeur « connecté » doit assurer la confidentialité, la disponibilité et l'intégrité des données. Il doit notamment protéger ses systèmes contre les risques de destruction accidentelle ou non autorisée, pertes accidentelles, erreurs techniques, falsifications, vols ou utilisations illicites, les modifications, copies, accès ou autres traitements non autorisés. Pour déterminer les mesures appropriées, il doit en particulier tenir compte du but du traitement de données, de la nature et de l'étendue du traitement de données, de l'évaluation des risques potentiels pour les personnes concernées et du développement technique. Ces mesures devront faire l'objet d'un réexamen périodique[88].

Il n'est pas rare que les entreprises sous-traitent l'aspect de la sécurité à des sociétés spécialisées. Dans ce cas, elles sont non seulement responsables du choix du mandant, mais également du contrôle de ce dernier ainsi que d'assurer que les exigences pour la sous-traitance de traitement de données (*infra* III.C) personnelles sont respectées. Indépendamment de l'aspect purement technique, une compagnie d'assurance faisant transiter un certificat LPP par l'employeur viole le principe de la sécurité[89].

B. Propre aux communications transfrontières de données personnelles

À la naissance de la LPD, Internet n'était que fort peu entré dans les foyers et très discret dans les entreprises. Aujourd'hui, la communication transfrontière de données est devenue une problématique centrale et incontournable en matière de traitement de données des employés par les employeurs. Il n'est par exemple pas rare de voir les services IT et comptabilité des entreprises être délocalisés en Inde, et plus généralement en Asie. En revanche, la publication de pages web, évidemment accessibles depuis le monde entier, ne constitue pas une communication de données à l'étranger, conformément à l'article 5 OLPD[90]. La révision en cours de la LPD apportera quelques légères modifications sur les modalités des communications transfrontières[91], mais sans rendre totalement désuet ce qui suit.

a) Niveau de protection adéquat

Sitôt qu'un employeur, public ou privé, envisage de communiquer des données personnelles à l'étranger notamment pour les analyser ou les stocker, il doit s'assurer qu'il

88 Art. 8 OLPD.

89 ATAF 2012/14 273 (298), c. 9.

90 Ordonnance relative à la loi fédérale sur la protection des données, RS 235.11.

91 Rapport explicatif du 21 décembre 2016 concernant l'avant-projet de loi fédérale sur la révision totale de la loi sur la protection des données et sur la modification d'autres lois fédérales, pp. 46 ss.

respecte les conditions posées par l'article 6 LPD. Ce dernier prévoit qu'aucune donnée personnelle ne peut être communiquée à l'étranger si la personnalité des personnes concernées devait s'en trouver gravement menacée, notamment du fait de l'absence d'une législation assurant un niveau de protection adéquat. En d'autres termes, il faut préalablement déterminer si le pays destinataire est reconnu posséder une telle législation par le PFPDT[92]. À relever que d'importants partenaires commerciaux de la Suisse, tels que la Chine, la Turquie, l'Inde et la Russie ne possèdent actuellement pas un niveau de protection adéquat, comme notamment l'Irak, la Syrie, le Tchad ou l'Afghanistan.

En ce qui concerne les États-Unis, la Suisse avait établi un « *U.S.-Swiss Safe Harbor Framework* »[93] similaire à celui de L'Union européenne (UE). Mais cet accord permettant de reconnaître à ce pays un niveau de protection adéquat est « tombé par ricochet »[94], puisque le célèbre « *U.S. – UE Safe Harbor Framework* »[95] liant les États-Unis et l'UE a été rendu caduc par l'arrêt « Schrems » de la Cour de justice de l'Union européenne (CJUE) du 6 octobre 2015[96]. L'UE reconnaît à nouveau l'adéquation des États-Unis aux règles européennes de la protection des données depuis le 12 juillet 2016, suite à la signature d'une nouvelle convention appelée « *U.S.-UE Privacy Shield Framework* »[97]. Quant à la Suisse, le Conseil fédéral a chargé en décembre 2015 le Secrétariat d'État à l'économie (SECO) de piloter les travaux visant à conclure un nouvel accord protégeant les droits de la personnalité des personnes concernées.

Les démarches ont abouti en janvier 2017 avec l'adoption d'un « *Bouclier de protection des données Suisse-États-Unis* ». Ce nouvel accord comprend des exigences similaires à celles obtenues par l'UE. La collaboration entre le Département du commerce américain et le PFPDT sera intensifiée. Pour obtenir une reconnaissance d'un niveau de protection adéquat par la Suisse, les entreprises américaines doivent s'engager à respecter les principes de protection des données par l'intermédiaire d'un dispositif géré et suivi par les autorités américaines. Ainsi, elles obtiennent une certification de conformité à ce « *U.S. –*

---

92 Art. 7 OLPD ; pays reconnus adéquats au 1.1.2017 par le PFPDT : Allemagne, Andorre, Autriche, Belgique, Bulgarie, Chypre, Croatie, Danemark, Espagne, Estonie, Finlande, France, Grèce, Guernesey, Hongrie, Île de Man, Îles Féroé, Irlande, Islande, Italie, Jersey, Lettonie, Liechtenstein, Lituanie, Luxembourg, Malte, Monaco, Norvège, Pays-Bas, Pologne, Portugal, République Tchèque, Roumanie, Royaume-Uni, Slovaquie, Slovénie, Suède, Canada, Argentine, Uruguay, Israël, Nouvelle-Zélande, pour plus de détails voir : https://www.edoeb.admin.ch/datenschutz/00626/00753/index.html?lang=fr.

93 http://2016.export.gov/safeharbor/.

94 https://www.edoeb.admin.ch/datenschutz/00626/00753/00970/01320/index.html?lang=fr.

95 http://2016.export.gov/safeharbor/eu/index.asp.

96 Arrêt CJUE C-362/14 Maximillian Schrems c. Data Protection Commissioner du 6 octobre 2015.

97 http://ec.europa.eu/justice/data-protection/international-transfers/eu-us-privacy-shield/index_en.htm ; https://www.privacyshield.gov/EU-US-Framework.

Swiss Privacy Shield Framework »[98]. Les entreprises suisses pourront ainsi effectuer des traitements avec de telles sociétés en se limitant à respecter les principes exposés ci-dessus. Par exemple, Microsoft Corporation, Google Inc., Amazon.com Inc., Facebook Inc. ont déjà adhéré à l'accord européen[99], contrairement à Apple et Samsung[100].

Pour les litiges, un organe de conciliation est à disposition pour traiter les conflits qui ne peuvent pas être réglés par les autres voies de recours. De plus, les personnes domiciliées en Suisse peuvent désormais adresser des demandes concernant le traitement de leurs données par les services de renseignements américains à un médiateur du Département d'État américain[101].

Au niveau européen, l'accord a fait l'objet de critiques de la part du groupe Article 29, regroupant les autorités nationales de protection des données. Il regrette « *le manque de règles spécifiques sur les décisions basées sur un traitement automatisé des données et l'absence d'un droit général d'opposition* », ainsi que l'absence de garanties plus strictes concernant l'indépendance et les pouvoirs du médiateur américain. Il relève aussi que le Bureau du directeur des services secrets n'a pris que l'engagement, figurant dans les annexes de l'accord, de ne pas conduire une collection en masse et systématique de données personnelles. Il regrette « *le manque d'assurances concrètes qu'une telle pratique n'ait pas lieu* »[102].

On se réjouit de voir si ces nouvelles règles, et surtout l'engagement de ne pas analyser systématiquement les données, éviteront à des Suisses, ou Européens, de se faire refouler à leur arrivée lors du passage de l'immigration, parce qu'ils ont évoqué l'éventualité de travailler aux États-Unis dans un e-mail ou sur Facebook[103].

b) Communications dans un pays possédant une législation adéquate

Si un pays figure sur la liste d'adéquation du PFPDT[104], il est possible de communiquer des données dans ce pays en respectant les mêmes principes que pour les traitements de données effectués exclusivement en Suisse (*supra* III.A). Toutefois, celui de la sécurité (*supra* III.A.4.g) mérite une attention soutenue lorsque les données sortent de Suisse, particulièrement pour les petites entreprises. Par exemple, le risque de perdre la disponibilité des données s'accentue considérablement selon le pays destinataire des

98 https://www.admin.ch/gov/fr/accueil/documentation/communiques.msg-id-65210.html.
99 https://www.privacyshield.gov/list.
100 État au 13.01.2017.
101 https://www.admin.ch/gov/fr/accueil/documentation/communiques.msg-id-65210.html.
102 http://www.europaforum.public.lu/fr/actualites/2016/07/article29-privacy-shield/index.html.
103 http://www.spiegel.de/lebenundlernen/schule/usa-einreise-abgelehnt-20-jaehrige-wegen-facebook-chat-abgewiesen-a-1046792.html.
104 Voir note 92.

données personnelles. Si un partenaire possède ses serveurs en Suisse et qu'il fait faillite, une petite entreprise individuelle pourra facilement s'adresser à un mandataire près de chez elle pour récupérer ses données dans un délai et pour un coût raisonnable. En revanche, il n'est pas certain que cette même entreprise réussisse à faire quoi que ce soit rapidement et pour un coût correspondant à ses moyens disponibles si l'entreprise destinataire a son siège en Estonie. En pareil cas, toutes les précautions prises contractuellement ne servent plus à grand-chose et la vie de l'entreprise pourrait être en péril faute de ne plus pouvoir effectuer son activité métier. Avoir des garanties contractuelles, y compris des clauses pénales, c'est bien, maîtriser véritablement, effectivement, ou à proximité, des données personnelles, c'est mieux. À quoi bon revendiquer l'application d'une clause pénale à une société en faillite en Estonie ou obtenir l'accès aux données plusieurs années après le blocage ?

Actuellement, la réalisation de ce type de danger peut paraître encore très « virtuelle ». Toutefois, les fournisseurs de services informatiques poussent de plus en plus leurs clients à héberger les données en dehors de l'entreprise. Pour s'en convaincre, il suffit de voir les récents produits de Microsoft, tels qu'Office 365 ou Windows 10. Ce modèle se généralise toujours plus rapidement, notamment dû à l'attractivité des coûts favorables de l'externalisation de l'hébergement, aspect sur lequel les entreprises s'arrêtent trop souvent, au détriment d'une solution interne, offrant suffisamment de garanties sécuritaires.

Certes, l'externalisation peut offrir aux petites entreprises individuelles de meilleures garanties en ce qui concerne la sécurité contre le hacking ou l'usure du matériel, mais elles ne devraient pas perdre de vue l'aspect de la disponibilité de leurs données.

c) Communications dans un pays ne possédant pas une législation adéquate

Si un pays ne figure pas dans la liste du PFPDT[105] et dans le cadre restreint des relations de travail, les entreprises peuvent communiquer des données à l'étranger si l'une de ces conditions est remplie :

– Conclusion d'un contrat contenant des clauses permettant d'assurer un niveau de protection adéquat à l'étranger[106]. Pour faciliter le travail des employeurs, l'UE[107], le Conseil de l'Europe[108] et le PFPDT[109] proposent des modèles. Il est également possible d'établir son propre contrat, devant au moins contenir l'identité de l'expéditeur et du destinataire des données, les catégories correspondant aux données

105 Voir note 92.

106 Art. 6 al. 2 let. a LPD.

107 http://ec.europa.eu/justice/data-protection/international-transfers/transfer/index_en.htm.

108 http://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016806ae511#search=contrat%2Dtype.

109 https://www.edoeb.admin.ch/datenschutz/00626/00743/00858/00859/index.html?lang=fr.

à communiquer, les buts de la communication, les catégories dans lesquelles sont classées les personnes concernées, les destinataires finaux des données et la durée de conservation de ces dernières. Les clauses doivent notamment permettre le respect des principes régissant la protection des données, garantir les droits des personnes concernées, à savoir le droit d'accès, le droit de rectification et le droit d'agir en justice; prévoir un mécanisme de contrôle, prévoir des mesures destinées à garantir la sécurité et la confidentialité lors de la communication de données sensibles ou de profils de la personnalité[110].

En plus de l'élaboration d'un contrat, à l'aide d'un modèle ou non, le PFPDT doit être informé du projet de communication à l'étranger. Pour ce faire, il suffit de lui envoyer une copie des garanties ou des règles de protection des données convenues avec le destinataire. En cas d'utilisation d'un modèle, seule la mention de son utilisation peut être communiquée. Par contre, s'il lui est apporté des modifications, elles doivent être envoyées en copie au PFPDT. Cette démarche doit s'effectuer avant la première communication, dès que possible en cas d'empêchement, et elle sera valable pour toutes les communications similaires suivantes. Elle peut s'effectuer par courrier postal ou par internet[111].

– Les employés concernés ont donné leur consentement pour une communication suffisamment délimitée[112]. Celui-ci n'est pas valable pour une communication régulière et systématique de données à l'étranger à des fins diverses et dans différentes situations[113]. L'ensemble des autres modalités relatives au consentement (*supra* III.A.3.b) doit évidemment être également respecté.
– L'employeur communique des données personnelles de ses employés à un tiers à l'étranger en vue de la conclusion ou l'exécution d'un contrat[114]. Par exemple, une entreprise envoie les données de monteurs de machines nécessaires à son client étranger afin que ce dernier puisse réserver les chambres d'hôtel et surtout les identifier lorsqu'ils viendront livrer la commande.
– La communication est, dans un cas particulier, indispensable soit à la sauvegarde d'un intérêt public prépondérant, soit à la constatation, l'exercice ou la défense d'un droit en justice[115]. Par exemple, cette condition a été jugée remplie par le PFPDT[116] pour la communication des données d'employés de banque aux États-Unis. En revanche, le

110 PFPDT, pp. 4 s.
111 PFPDT, p. 7.
112 Art. 6 al. 2 let. b LPD.
113 PFPDT, p. 5.
114 Art. 6 al. 2 let. c LPD.
115 Art. 6 al. 2 let. d LPD.
116 WYLER, p. 344.

Tribunal fédéral a décidé qu'elle n'était pas remplie pour les avocats d'une banque[117]. Plus récemment, des instances cantonales ont interdit la communication de données d'employés de banque en jugeant que la condition de l'intérêt public prépondérant n'était pas remplie[118].

- La communication est nécessaire pour protéger la vie ou l'intégrité corporelle d'un employé[119] ; on peut imaginer que l'employeur doive rapidement envoyer des données personnelles d'un employé victime d'un accident lors d'une intervention chez un client à l'étranger. De même lorsqu'il s'agit de rechercher des personnes disparues dans une zone de conflit ou dans une région qui a subi une catastrophe naturelle[120].
- L'employé a rendu les données accessibles à tout un chacun et il ne s'est pas opposé formellement au traitement[121]. Cependant, cette condition doit être lue en parallèle avec les exigences imposées par l'article 328b CO (*supra* III.A.4.a) ; c'est-à-dire que l'employeur ne peut, par exemple, pas communiquer à l'étranger des données sans lien avec la relation de travail, récoltées sur un réseau social, alors que cette disposition ne permet en aucun cas de les traiter[122].
- La communication a lieu au sein d'une même personne morale ou société ou entre des personnes morales ou sociétés réunies sous une direction unique, dans la mesure où les parties sont soumises à des règles de protection des données qui garantissent un niveau de protection adéquat[123]. Autrement dit, les groupes de sociétés doivent remplir au moins les conditions applicables aux personnes privées traitant des données figurant dans la Convention STE 108 et dans son Protocole additionnel[124]. Le caractère contraignant des règles en vigueur dans les groupes de sociétés doit être garanti. Il peut être conféré par exemple par une décision du conseil d'administration et des audits[125]. Comme pour la première condition, le PFPDT doit être informé des règles internes adoptées par des groupes internationaux de sociétés de la même manière que lors d'élaboration d'un contrat.

---

117 TF 4A_83/2016 du 6 octobre 2016, c. 2.

118 ZR 115/2016, p. 117, arrêt du 8 février 2016 n'ayant pas fait l'objet d'un recours au TF ; http://www.24heures.ch/vaud-regions/Banquier-sauve-des-griffes-americaines/story/23588487.

119 Art. 6 al. 2 let. e LPD.

120 Rapport explicatif du 21 décembre 2016 concernant l'avant-projet de loi fédérale sur la révision totale de la loi sur la protection des données et sur la modification d'autres lois fédérales, p. 49.

121 Art. 6 al. 2 let. f LPD.

122 Conseil fédéral, p. 58.

123 Art. 6 al. 2 let. g LPD.

124 RS 0.235.11.

125 PFPDT, p. 7.

C. Propre à la sous-traitance

Un traitement de données personnelles peut être confié à un tiers pour autant qu'une loi ou une convention le prévoie, que seuls les traitements que le mandant est en droit d'effectuer lui-même soient traités et qu'aucune obligation légale ou contractuelle de garder le secret ne l'interdise. Le mandant doit en particulier s'assurer que le tiers garantisse la sécurité des données[126].

L'usage d'un Cloud ou d'un prestataire externe de gestion des ressources informatiques, de même que les échanges avec une succursale ou une société du même groupe doivent répondre à ces exigences[127]. Pour la sécurité, il ne suffit pas de se fier aux assurances du prestataire, mais d'exercer des vérifications concrètes et régulières. Le mandataire doit évidemment respecter les exigences légales figurant dans la LPD et son ordonnance (*supra* III.A.4.g)[128] ou les règles cantonales.

Pour l'heure, le sous-traitant peut lui-même sous-traiter sans avoir de modalités particulières à respecter, excepté les principes généraux. À l'avenir, il devra sûrement obtenir l'accord écrit du mandant[129].

Bien évidemment, sitôt que la sous-traitance entraîne une communication de données à l'étranger, les règles spécifiques à ce traitement doivent être respectées (*supra* III.B).

Concrètement, les fiduciaires, les avocats, les notaires, les médecins, ou toute autre profession soumise à un secret doivent faire preuve d'une vigilance soutenue lors du choix de leur réseau et outils informatiques. Il leur est quasiment impossible de respecter leur secret s'ils s'équipent de produits standards et répandus ou ne prennent pas des mesures particulières[130].

Tous les cantons offrent des règles similaires, mais pouvant spécifier une ou deux petites modalités différentes.

IV. Conclusions

Le numérique a envahi notre société y compris le monde du travail. La vigilance qu'exigeait le monde du papier est sans comparaison avec celle dont doivent faire preuve

126 Art. 10a LPD.
127 DUNAND, N 22 *ad* art. 328b CO, p. 324.
128 FANTI, p. 76 ; FANTI, BYOD, p. 186.
129 Rapport explicatif du 21 décembre 2016 concernant l'avant-projet de loi fédérale sur la révision totale de la loi sur la protection des données et sur la modification d'autres lois fédérales, p. 50.
130 HEINZELMANN, p. 368 ; BOHNET/MARTENET, N 375, p. 161.

les employeurs aujourd'hui. Les exigences en matière de protection des données n'ont pas diminué, bien au contraire. Les risques sont encore régulièrement sous-estimés, car souvent trop abstraits aux yeux des dirigeants et les mesures trop coûteuses. La constatation d'un traitement illicite de données apparaîtra de manière croissante, lors des licenciements, tant du côté de l'employeur que de l'employé, ou d'action en responsabilité. Sans compter qu'au vu de l'évolution de l'opinion publique, toujours plus sensible à la problématique de la protection des données, se posera la question des risques en termes d'image pour une entreprise. Les sociétés telles que Nike ou Apple n'ont-elles pas été fortement ébranlées lorsque les conditions de travail de leurs sous-traitants ont été dénoncées ?

Les risques diminueront drastiquement lorsque les employeurs acquerront le réflexe de se poser des questions simples et basiques, mais terriblement efficaces : ces données personnelles sont-elles indispensables pour juger l'aptitude ou exécuter le contrat de travail ? Permettent-elles réellement d'atteindre ces buts ? Ne pourrais-je pas les demander directement à l'employé au lieu de passer par un tiers ? Ne devrais-je pas renvoyer le tiers poser la question directement à l'employé ? Combien de temps en ai-je besoin pour ce faire ? Suis-je suffisamment protégé contre les risques de vols, indisponibilité et rupture de confidentialité ?

Ces quelques réflexes devraient assez vite et facilement orienter employeurs et employés à appréhender la conformité d'un traitement (ou non) selon les règles de la protection des données. Avant l'ère du numérique, il n'était pas venu à l'idée de beaucoup d'employeurs de mandater un détective pour observer la vie privée d'un candidat à un emploi, alors que maintenant, il est devenu d'usage de récolter toutes les traces possibles que ce dernier a laissées sur le net.

La révision de la LPD devrait contribuer à améliorer la prise de conscience, même si cela reste difficile lorsque les entreprises traversent une crise. Quoi qu'il en soit, les changements n'interviendront pas sans de gros efforts de sensibilisation ; www.thinkdata.ch est un site qui se prête très bien à cette démarche.

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.

AUBERT GABRIEL, La protection des données dans les rapports de travail, *in* : Gabriel Aubert et al., Journée 1995 de droit du travail et de la sécurité sociale, Zurich 1999, pp. 145-191.

BOHNET FRANÇOIS/MARTENET VINCENT, Droit de la profession d'avocat, Genève 2009.

CONSEIL FÉDÉRAL, Cadre juridique pour les médias sociaux, Rapport du Conseil fédéral en réponse au postulat Amherd 11.3912 du 29 septembre 2011, Berne 2013.

DU PASQUIER SHELBY R./OBERSON XAVIER/FISCHER PHILIPP, Transmission d'informations à l'étranger, Bâle 2014.

DUNAND JEAN-PHILIPPE, Commentaire de l'art. 328b CO, *in* : Jean-Philippe Dunand/Pascal Mahon (éds.), Commentaire du contrat de travail, Berne 2013.

FANTI SÉBASTIEN, Cloud computing : opportunités et risques pour les avocats, *in* : Revue de l'avocat, 2013, pp. 74 ss.

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 (cité : FANTI, BYOD).

FLUECKIGER CHRISTIAN, Dopage, santé des sportifs professionnels et protection des données médicales, Genève 2008.

FLUECKIGER CHRISTIAN, La googlelisation des employés respecte-t-elle les principes de la protection des données, *in* : Jean-Philippe Dunand/Pascal Mahon (éds.), Internet au travail, Genève/Zurich/Bâle 2014, pp. 73 ss (cité : FLUECKIGER, Googlelisation).

GRAND CARMEN, Protection des données dans les rapports de travail et dans les assurances, *in* : Colloques et journées d'étude organisées par l'IRAL, Lausanne 2002, p. 52.

GROUPE DE TRAVAIL « ARTICLE 29 » SUR LA PROTECTION DES DONNÉES, institué par la directive 95/46/CE, Avis 05/2014 sur les Techniques d'anonymisation, adopté le 10 avril 2014.

HEINZELMANN REGULA, Maintien du secret professionnel, Prudence face aux « clouds » et aux réseaux sociaux, *in* : TREX – L'expert fiduciaire, 2015, pp. 368 ss.

MANAÏ DOMINIQUE, Droits du patient face à la biomédecine, Berne 2013.

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

PRÉPOSÉ FÉDÉRAL À LA PROTECTION DES DONNÉES ET À LA TRANSPARENCE, La communication de données à l'étranger en 24 questions, état septembre 2014.

PRÉPOSÉ FÉDÉRAL À LA PROTECTION DES DONNÉES ET À LA TRANSPARENCE, Rapport d'activités n° 5 (1997/1998), Berne 1998 (cité : PFPDT, Rapport).

PRÉPOSÉ FÉDÉRAL À LA PROTECTION DES DONNÉES ET À LA TRANSPARENCE, Guide pour le traitement des données personnelles dans le secteur du travail, état octobre 2014 (cité : PFPDT, Guide).

RÜTSCHE BERNHARD, Was sind öffentliche Aufgaben ?, *in* : Recht, Zeitschrift für juristische Weiterbildung und Praxis, 4/13, pp. 153-162.

RÜTSCHE BERNHARD, Surveillance de la protection des données dans les hôpitaux, *in* : Digma, 6/2012 (cité : RÜTSCHE, Surveillance).

WILDHABER ISABELLE/HÄNSENBERGER SILVIO, Internet am Arbeitsplatz, *in* : ZBJV, 152/2016, pp. 307 ss.

WYLER REMY/HEINZER BORIS, Droit du travail, 3e édition, Berne, 2014.

ZEN-RUFFINEN PIERMARCO, Droit administratif, partie générale et éléments de procédure, Neuchâtel 2011.

AURÉLIEN WITZIG

Actions et procédure

Sommaire Page

I. Actions 26
A. Les parties à l'action 26
1. Le demandeur 26
2. Le défendeur 27
B. Les sortes d'actions 28
1. Les actions civiles 29
a) Les actions au fond 29
aa) Les actions protectrices 29
bb) Les actions défensives 32
cc) Les actions réparatrices 34
dd) Les moyens de contre-attaque de l'employeur 36
b) Les mesures provisionnelles 38
2. Les actions pénales 38
a) L'inexactitude et l'incomplétude des renseignements fournis, ainsi que la mauvaise exécution du droit d'accès 39
b) L'inexécution du devoir d'information lors de la collecte de données 40
c) La non-déclaration ou la mauvaise déclaration de fichiers au préposé fédéral à la protection des données, ainsi que le refus de collaboration ou la mauvaise collaboration avec ce dernier 40
d) La violation du devoir de discrétion 40
3. Les actions administratives 41

II. Procédure 42
A. Compétence 42
1. La compétence territoriale 42
2. La compétence matérielle 43
B. Les sortes de procédures 44
1. La procédure ordinaire 44
2. La procédure simplifiée 44
3. Coût de la procédure 45

Bibliographie 45

Le droit de la protection des données au travail instaure un régime juridique spécifique, étudié par les autres contributions de cet ouvrage. Dans cet article, il s'agit de se concentrer sur ce qui permet de rendre juridiquement effectifs les principes ainsi énoncés : l'action en justice.

En effet, comme de nombreux autres domaines du droit suisse, le droit de la protection des données est principalement sanctionné lorsqu'une personne, qui s'estime victime d'une violation, porte sa réclamation devant un juge. Certes, le Préposé à la protection des données possède la faculté de s'autosaisir de certaines situations qui lui paraissent appeler une intervention administrative[1]. Mais en dehors de ces cas – somme toute assez rares par rapport à l'ensemble des données traitées quotidiennement dans le monde du travail –, le détour par le juge est nécessaire. La doctrine a souligné, à regret, combien l'effectivité de la loi se trouve diminuée dans une telle configuration, notamment en raison des coûts d'une action en justice, de son incertitude et du faible niveau des compensations financières qui sont généralement octroyées[2].

La mise en œuvre procédurale de prétentions juridiques est assujettie à un certain nombre de règles, dont la plupart ressortissent au droit général de la procédure judiciaire et administrative. Nous nous attacherons ici à mettre en évidence les spécificités induites par la protection des données au travail. Comme y invite le titre de notre article, seront dans l'ordre étudiées les ***actions*** (**I**), puis la ***procédure*** (**II**).

I. Actions

Lorsqu'un litige en matière de protection des données au travail ne se résout pas à l'amiable, les personnes concernées doivent envisager le recours au juge. Procéder devant le juge implique, au préalable, de déterminer les ***parties à l'action*** (**A**). Pour formuler leurs conclusions, les parties doivent ensuite choisir l'une des ***sortes d'actions*** admissibles (**B**).

A. Les parties à l'action

Qui peut être ***demandeur*** à l'action (**1**) et contre quel ***défendeur*** (**2**) ?

1. Le demandeur

Il ne fait guère de doute que le ***travailleur*** a un intérêt à agir à l'égard des données qui le concernent, comme toute personne faisant l'objet d'un traitement de données au sens de la loi sur la protection des données (LPD). Il a également un intérêt à agir lorsqu'il prétend que sa personnalité est ou a été violée, au sens des articles 328 ou 328b du code des

[1] Cf. *infra* I. B. 3.

[2] Cf. MEIER, N 1718, p. 563, citant d'autres auteurs et montrant, indirectement, l'intérêt que la reconnaissance procédurale d'une « action de groupe » pourrait avoir en la matière.

obligations (CO), voire au sens des articles 28 et suivants du Code civil (CC). La qualité de partie doit donc lui être reconnue dans toutes ces situations.

Plus délicate est la position du ***postulant***, c'est-à-dire de la personne qui a, par hypothèse, envoyé un dossier à un employeur potentiel dans le cadre d'une procédure de recrutement, ou même rencontré cet employeur dans le cadre d'un entretien. La doctrine reconnaît au postulant la faculté d'agir en matière de protection des données[3]. Cette solution convainc en ce sens que les conséquences d'un mésusage des données du postulant peuvent tout autant lui porter atteinte que s'il était devenu employé. Par ailleurs, la LPD elle-même ne distingue pas, sur ce point, entre les positions contractuelles des personnes dont les données sont traitées.

Un ***syndicat*** peut-il agir en lieu et place d'un travailleur ou en concours avec lui ? Selon l'article 89 alinéa 1 du code de procédure civile (CPC), les « associations et les autres organisations d'importance nationale ou régionale qui sont habilitées aux termes de leurs statuts à défendre les intérêts d'un groupe de personnes déterminé peuvent, en leur propre nom, agir pour l'atteinte à la personnalité des membres de ce groupe ». Le CPC limite toutefois les sortes d'actions ouvertes à ces organisations : ces dernières ne peuvent agir qu'en interdiction, en cessation ou en constatation du caractère illicite d'une atteinte (art. 89 al. 2 CPC)[4]. Ainsi, ces organisations ne peuvent pas conclure à des réparations matérielles ou morales en lieu et place du travailleur concerné[5]. Il faut souligner que le CPC, en son article 89 alinéa 3, réserve expressément la capacité pour agir des associations lorsqu'elle est prévue par une loi spéciale[6]. La LPD ne prévoit toutefois pas une telle possibilité, dès lors que son article 33 alinéa 1 se borne à prévoir que « les voies de droit sont régies par les dispositions générales de la procédure fédérale ».

2. Le défendeur

L'***employeur***, en tant que maître du fichier et personne tenue d'une obligation de protéger la personnalité de ses salariés, est le défendeur naturel à l'action intentée par le travailleur en matière de protection des données.

Comme l'employeur est responsable de ses ***organes*** (s'il en possède en tant que personne morale), de ses ***auxiliaires*** et de ses ***employés*** (sauf s'il prouve qu'il a pris tous les soins commandés par les circonstances pour détourner un dommage de ce genre ou que sa diligence n'eût pas empêché le dommage de se produire), il peut être attaqué directement,

---

3 STREIFF/VON KAENEL/RUDOLPH, N 19 *ad* art. 328b CO, p. 624 ; DUNAND, N 109 *ad* art. 328b CO.

4 Cf. DIETSCHY, N 727, pp. 349 ss ; DONATIELLO, pp. 825 ss ; DUNAND, N 67 *ad* art. 328 CO. Sur ces actions, cf. *infra* I. B. 1. a. bb.

5 BRUNNER/BÜHLER/WAEBER/BRUCHEZ, N 17 *ad* art. 328 CO, p. 151 ; DIETSCHY, N 728, p. 351 ; DONATIELLO, pp. 832 s ; DUNAND, N 67 *ad* art. 328 CO.

6 DIETSCHY, N 729 ss, pp. 351 ss.

même si ce sont ses organes, ses auxiliaires ou ses employés qui sont à l'origine de la violation. La responsabilité de l'employeur pour ses organes se fonde sur l'article 55 CC, pour ses auxiliaires sur l'article 101 CO, pour ses employés sur l'article 55 CO.

Les fautes commises par les organes d'une personne morale engagent, au surplus, la responsabilité personnelle de leurs auteurs (art. 55 al. 3 CC). Les membres des organes de l'employeur-personne morale peuvent donc être assignés en justice. Il en va de même lorsque la responsabilité délictuelle d'un employé est directement engagée à l'égard de l'un de ses collègues sur le fondement de l'article 41 CO. Toutefois, en pratique, il paraît peu stratégique de la part du travailleur, sauf cas particulier, de multiplier ses adversaires.

Qu'en est-il des ***tiers*** à qui serait confié le traitement de données personnelles des travailleurs ? Selon le Préposé fédéral à la protection des données, « il incombe au maître du fichier, c'est-à-dire à la personne qui décide du but et du contenu du fichier (art. 3i LPD), de veiller à ce que les dispositions sur la protection des données soient respectées. Cette règle s'applique également lorsque le traitement de données est confié à un tiers (à un centre de calcul, par exemple). Le mandant est tenu de veiller à ce qu'il ne soit pas effectué de traitement autre que celui qu'il est lui-même en droit d'effectuer (art. 10a al. 1a LPD)[7] ».

Ainsi, même lorsqu'il confie l'exploitation du fichier à un tiers, l'employeur reste responsable à l'égard du travailleur et peut donc se voir attaqué par ce dernier en cas de violation de prescriptions de la protection des données au travail[8].

B. Les sortes d'actions

Le droit de la protection des données prévoit un certain nombre de principes[9]. Quelles violations de ces principes peuvent être sanctionnées par une action en justice et de quelle manière ?

Les trois ordres de juridiction peuvent être sollicités, par des actions ***civiles*** (**1**), des actions ***pénales*** (**2**) ou des actions ***administratives*** (**3**).

---

7 Préposé fédéral à la protection des données et à la transparence, Guide pour le traitement des données personnelles dans le secteur du travail, octobre 2014, N 2.1.3, p. 5.

8 MEIER, N 139, p. 433 ; DUNAND, N 107 *ad* art. 328b CO.

9 Pour mémoire : le traitement des données doit être licite (art. 4 LPD), les données doivent être exactes (art. 5 LPD), la communication transfrontière de données doit respecter certaines conditions (art. 6 LPD), les données doivent être sécurisées (art. 7 LPD), l'accès aux données doit être garanti (art. 8 – 10 LPD), le traitement des données par un tiers doit respecter certaines conditions (art. 10a LPD), le fichier doit être déclaré (art. 11a LPD), la personnalité doit être respectée (art. 12-13 LPD), l'information doit être correctement donnée (art. 14 LPD).

1. Les actions civiles

Les actions civiles permettent de rendre effective la protection de la personnalité du travailleur en matière de protection des données. Elles s'exercent généralement ***au fond*** (**a**). Dans certains cas, des ***mesures provisionnelles*** peuvent également être requises (**b**).

a) Les actions au fond

Les actions au fond pertinentes ici sont les actions ***protectrices*** (**aa**), les actions ***défensives*** (**bb**) et les actions ***réparatrices*** (**cc**)[10]. Face à ces actions, l'employeur possède des moyens procéduraux de ***contre-attaque*** (**dd**).

aa) Les actions protectrices

Nous appelons « actions protectrices » les actions que peut intenter le travailleur indépendamment de toute violation effective de sa personnalité[11]. En d'autres termes, le demandeur à une telle action ***n'a pas à justifier d'un intérêt*** pour motiver sa demande[12]. Les actions protectrices sont l'action en exécution du droit d'accès aux données et l'action en rectification des données inexactes.

Disons-le d'emblée, il existe une réserve à l'admission absolue de ces deux actions : l'***abus de droit***. Ces actions ne peuvent être exercées par le travailleur dans un but étranger à la protection des données, dans l'unique dessein de nuire à l'employeur[13].

Concrètement, le Tribunal fédéral envisage de « considérer comme contraire à son but et donc abusive l'utilisation du droit d'accès dans le but exclusif d'espionner une (future) partie adverse et de se procurer des preuves normalement inaccessibles »[14]. Il prend comme exemple « une requête qui ne constituerait qu'un prétexte à une recherche indéterminée de moyens de preuve (*fishing expedition*) ». Il y oppose la requête de l'employé visant à obtenir les données qui le concernent en vue d'une éventuelle action en dommages-intérêts contre le maître du fichier, laquelle requête n'est, en soi, pas abusive[15].

Le raisonnement du Tribunal fédéral paraît ici quelque peu ***contradictoire***. En effet, de deux choses l'une : soit le droit d'accès n'exige pas la justification d'un quelconque intérêt, et dès lors il ne saurait être exercé abusivement que si le demandeur a déjà connaissance

---

10 Pour les deux dernières branches de cette classification, cf. MEIER, pp. 566 et 578.

11 Cf. MEIER, N 968, pp. 362 s. et N 1725, p. 565 ; DUNAND, N 112 *ad* art. 328b CO.

12 ATF 141 III 119, c. 7.1.1. La formulation que nous avons employée est empruntée à la délibération n° 80-10 du 1er avril 1980 de la Commission nationale française informatique et libertés, publiée au JORF, 29 mai 1980, p. 1319.

13 ATF 141 III 119, c. 7.1.1 ; TF 4A_36/2010 du 20 avril 2010, c. 3.1.

14 ATF 138 III 425, c. 5.5 ; ATF 141 III 119, c. 7.1.1.

15 ATF 138 III 425, c. 5.6 ; ATF 141 III 119, c. 7.1.1.

du contenu des données le concernant, ou n'a strictement aucun intérêt à le connaître ; soit le droit d'accès exige la démonstration d'un intérêt et, dès lors, le demandeur devrait en apporter la preuve. Une telle exigence ne correspondrait toutefois pas à la *ratio legis* de l'article 8 LPD.

Le risque de *fishing expedition,* tant redouté par le Tribunal fédéral, peut être écarté de deux autres manières : premièrement, les informations que l'employeur peut être requis de transmettre au travailleur doivent correspondre à la définition des données personnelles selon la LPD, ce qui limite leur domaine ; en second lieu, comme nous le verrons juste après, la conclusion en exécution du droit d'accès est une conclusion au fond et non une simple conclusion préalable, ce qui signifie qu'elle n'a pas une visée directement probatoire.

Ce préalable étant acquis, passons à l'observation du régime de chacune de ces deux actions :

L'action en exécution du droit d'accès aux données

Cette action découle directement de l'article 8 LPD. Si l'employeur n'autorise pas un travailleur à consulter son dossier ou refuse sans motifs légitimes de lui en communiquer le contenu, le travailleur peut s'adresser au juge afin qu'il ordonne à l'employeur de fournir cet accès[16].

Dans la pratique, on voit souvent un travailleur conclure à l'exécution du droit d'accès à titre préalable dans le cadre d'une procédure prud'homale. Est-ce juridiquement admissible ?

L'action en exécution du droit d'accès est une ***action au fond***[17]. À ce titre, elle doit faire l'objet d'une conclusion spécifique de la part du demandeur, au même titre que ses autres prétentions au fond. En tant que tel, le droit d'accès ne relève donc pas de la procédure probatoire, même si le travailleur pourrait avoir un intérêt stratégique à obtenir la communication des données le concernant avant d'engager un procès au fond. Comme le suggère le Tribunal fédéral, ce pourrait être le cas pour déterminer la possibilité d'intenter une des actions réparatrices qu'octroie la protection des données[18]. Ce pourrait être également le cas pour décider de l'opportunité de réclamer une indemnité pour licenciement abusif ou licenciement immédiat injustifié. En effet, le travailleur supporte juridiquement la charge de la preuve alors qu'il ignore parfois les motifs précis de son licenciement, l'employeur ne les lui ayant pas communiqués ou les lui ayant communiqués

16 MEIER, N 1099 ss, pp. 396 ss ; DUNAND, N 112 *ad* art. 328b CO.

17 Au sujet du droit d'accès, cf. la contribution de MARIE MAJOR, « Le droit d'accès de l'employé à son dossier personnel », dans le présent recueil, pp. 287 ss.

18 Cf. ATF 141 III 119, c. 7.1.1, traité *supra* ; concernant les actions réparatrices, cf. *infra* I. B. 1. a. cc.

imparfaitement. Il n'en demeure pas moins qu'une telle action relève d'une protection matérielle et non d'une possibilité procédurale. Toutefois, dès lors qu'il est demandé dans les conditions légales de la LPD, l'accès doit être accordé indépendamment de l'usage ultérieur qui pourra être fait des données. Il s'agit d'une conséquence, certes non prévue par le législateur, mais intrinsèque au droit d'accès lui-même.

L'action en exécution du droit d'accès peut être demandée à titre de ***mesure provisionnelle***[19].

Pour autant que les conditions jurisprudentielles posées en regard de l'article 86 CPC soient remplies, l'action en exécution du droit d'accès pourrait faire l'objet d'une ***action partielle***, encore qu'il s'agirait vraisemblablement d'une action partielle improprement dite (*unechte Teilklage*)[20] et que sa mise en œuvre ne revêtirait pas un intérêt pratique manifeste.

Inversement, la mise en œuvre de l'action en exécution du droit d'accès ne constitue pas un préalable nécessaire à une action en protection de la personnalité[21].

Le demandeur qui intente une action en exécution du droit d'accès peut conclure non seulement à pouvoir prendre connaissance des données le concernant, mais également, en principe, à ce qu'une ***copie*** de ces données lui soit remise[22]. De manière plus générale, il est possible de conclure en faveur de l'obtention de chacune des différentes modalités du droit d'accès (confirmation de l'existence d'un fichier, consultation *in situ*, transmission orale et écrite des données, communication relative au but et aux modalités de traitement du fichier, etc.)[23].

L'action en rectification des données inexactes

Cette action est directement fondée sur l'article 5 alinéa 2 LPD[24], qui énonce que « toute personne concernée peut requérir la rectification des données inexactes ».

Ainsi, lorsque, consultant son dossier, le travailleur constate l'inexactitude des données le concernant, il peut en demander la rectification[25].

---

19 TF 4P.293/2006 du 9 février 2007, c. 4.4. Cf. *infra*, I. B. 1. b.

20 Sur ce concept, cf. BOPP/BESSENICH, N 5 *ad art.* 86 CPC, p. 781.

21 MEIER, N 969, p. 363 ; DUNAND, N 112 *ad* art. 328b CO.

22 ATF 141 III 119, c. 7.1.4 et 7.5.

23 Sur le principe et pour les bases légales concernant ces différents éléments, cf. AUBERT, Modalités.

24 MEIER, N 1725, p. 565 ; DUNAND, N 109 *ad* art. 328b CO.

25 BRUNNER/BÜHLER/WAEBER/BRUCHEZ, N 7 *ad* art. 328b CO, p. 157.

Le Tribunal fédéral précise toutefois que la procédure prévue par la LPD ne saurait avoir pour objet de remettre en cause, après la fin des rapports de travail, les différentes évaluations faites par l'employeur au sujet des prestations de l'employé. Ainsi, l'intéressé ne peut requérir que la rectification de ***données de fait*** qui se révèlent inexactes[26]. L'espèce qui a donné lieu à l'énonciation de cette règle concernait un cas de droit public. On peut néanmoins en retirer la règle générale selon laquelle il appartient au juge d'examiner, dans le dossier du travailleur, quelles sont les données purement factuelles dont l'exactitude est contestée.

Dans l'hypothèse où ni l'exactitude, ni l'inexactitude d'une donnée ne peuvent être prouvées, une note au dossier faisant état du caractère litigieux des mentions contestées doit être jointe[27], à l'instar de ce que prévoit l'article 15 alinéa 2 LPD[28].

À notre sens, la décision de joindre la mention du caractère litigieux d'une donnée peut être prise par le juge ***même en l'absence de conclusion spécifique*** sur ce point par le demandeur, dès lors que ce dernier a conclu à la rectification de la donnée qu'il considérait inexacte. En effet, la condamnation à l'ajout d'une telle mention revient à accorder au demandeur moins que ce qu'il a demandé, mais non pas davantage, ni autre chose. Dans le doute, le demandeur sera toutefois bien inspiré de réclamer, à titre principal, la rectification des données inexactes (en précisant d'ailleurs dans la conclusion elle-même la rectification qu'il demande) et, à titre subsidiaire, l'ajout de la mention du caractère litigieux de la donnée.

bb) Les actions défensives

L'action en interdiction de l'atteinte

L'action en interdiction de l'atteinte est prévue par l'article 28a CC, auquel renvoie l'article 15 LPD.

Ce dernier article précise une application particulière en matière de protection des données, à savoir la possibilité pour le demandeur de requérir que le traitement des données soit interdit, ou que la communication à des tiers soit interdite (LPD, art. 15 al. 1 2e phrase), notamment à titre préventif[29].

Ce type d'action a connu récemment un certain retentissement en droit du travail, lorsque des employés de banque ont demandé au juge qu'il soit interdit à leur employeur de

[26] TF 1A.295/2005 du 29 mars 2006, c. 2.4.
[27] TF 1A.295/2005 du 29 mars 2006, c. 2.4.
[28] Cf. *infra* : action en mention du caractère litigieux.
[29] MEIER, N 1738, p. 568.

transmettre des données les concernant à des autorités étrangères. Le point de savoir si l'employeur peut se voir contraint de refuser la transmission de ces données relève du droit de fond et déborde par conséquent le cadre de cet article. Notons tout de même que les juges ont généralement considéré qu'il n'existait pas d'intérêt prépondérant susceptible d'autoriser la transmission des données des salariés à l'étranger[30].

Il est conseillé de préciser dans les conclusions de la demande en justice, en sus du principe de l'interdiction, les ***actions concrètes*** que le lésé veut voir être interdites (par exemple, interdiction d'exploiter les données, interdiction de les transmettre à des tiers, en particulier tel tiers désigné, etc.). À notre sens, ces interdictions précises, mentionnées à titre d'exemple, peuvent être introduites par l'adverbe « notamment ». Dans une telle configuration, les conclusions répondent selon nous aux critères de précision requis par le droit de procédure[31].

L'action en cessation de l'atteinte

À côté de l'action en interdiction de l'atteinte, il faut faire une place à l'action en cessation de l'atteinte, prévue par les mêmes articles.

En outre, le travailleur peut requérir que les données soient détruites (art. 15 al. 1 LPD).

Comme pour l'action en interdiction de l'atteinte, les conclusions du demandeur gagnent selon nous à mentionner les actions concrètes que ce dernier souhaite que le juge ordonne.

Pour l'action en cessation de l'atteinte, comme d'ailleurs pour l'action en interdiction de l'atteinte, il est conseillé de demander que la condamnation soit assortie de la menace des peines de l'article 292 du Code pénal (CP) en cas d'insoumission[32].

L'action en constatation du caractère illicite de l'atteinte

L'action en constatation de l'atteinte est prévue par l'article 28a CC, auquel renvoie l'article 15 alinéa 1 1re phrase LPD.

Dès lors qu'entre le moment de l'introduction de l'instance et le moment du jugement, l'atteinte peut avoir soit persisté soit cessé, il est conseillé au travailleur de ***grouper les trois actions*** que nous venons de présenter : il conclura ainsi à la fois en interdiction de l'atteinte – pour le cas où l'atteinte ne se serait pas encore produite – et en cessation de

---

30 Cf. *inter alia :* TAF B-7969/2015 du 16 mars 2016 ; TAF B-7773/2015 du 16 mars 2016 ; CJ-GE ACJC/1529/2015 du 11 décembre 2015, *in* : RSDA 2015, p. 407. Pour une synthèse, cf. THEVENOZ/EMMENEGGER/PODA/KISSLING, pp. 210-211.

31 Au sujet de la précision des conclusions, cf. par exemple : SCHEIWILLER, N 166-167, p. 74.

32 Du même avis : MEIER, N 1742, p. 569.

l'atteinte – pour le cas où l'atteinte perdurerait –, ainsi que, subsidiairement, en constatation du caractère illicite de l'atteinte – dans l'hypothèse où l'atteinte aurait définitivement cessé[33].

L'action en mention du caractère litigieux de la donnée

Une telle action doit s'envisager lorsque ni l'exactitude, ni l'inexactitude d'une donnée personnelle ne peuvent être établies[34]. Le demandeur, ou le défendeur à titre de demande reconventionnelle (par exemple l'employeur lorsque le travailleur a conclu à la rectification d'une donnée), peut alors requérir que l'on ajoute à la donnée la mention de son caractère litigieux (art. 15 al. 2 LPD).

Comme nous l'avons indiqué précédemment, il peut être judicieux de conclure à la mention du caractère litigieux de la donnée subsidiairement à une conclusion en rectification de données inexactes[35].

L'action en communication ou en publication de la mesure ou du jugement

Le travailleur peut demander que la rectification ou la destruction des données, l'interdiction de la communication, à des tiers notamment, la mention du caractère litigieux ou la décision soient communiquées à des tiers ou publiées (art. 15 al. 3 LPD).

Une telle demande peut être formulée ***même si*** l'employeur a accepté de rectifier des données concernant le travailleur et de les revêtir de la mention du caractère litigieux.

cc) Les actions réparatrices

Les actions réparatrices sont plus intéressantes financièrement lorsque le demandeur obtient gain de cause. De ce fait, elles seront privilégiées par les demandeurs dans toutes les hypothèses où les conditions en seront remplies.

Les actions réparatrices en matière de protection des données au travail sont les suivantes :

L'action en dommages-intérêts

Cette action est prévue par l'article 28a CC, auquel renvoie l'article 15 alinéa 1 1re phrase LPD[36].

---

33 Du même avis : MEIER, N 1739, pp. 568-569.

34 TF 1A.295/2005 du 29 mars 2006, c. 2.4 ; ArbG/ZH du 26 juin 2006, *in* : JAR 2007, p. 524, c. 3 ; MEIER, N 1756 ss, pp. 572 ss.

35 Cf. *supra* I. B. 1. a. aa.

36 Cf. MEIER, N 1735 ss, pp. 567 ss ; DUNAND, N 109 *ad* art. 328b CO.

Une action en dommages-intérêts est possible sur un fondement ***contractuel*** ou ***délictuel***. Ainsi, le travailleur peut demander des dommages-intérêts en raison du préjudice qu'il subit et qui résulte d'une atteinte à sa personnalité du fait d'un traitement illicite de données dont l'employeur est responsable[37]. Selon un principe général du droit suisse, un même acte peut engager à la fois la responsabilité contractuelle et la responsabilité délictuelle de son auteur. Le travailleur dispose alors d'un concours alternatif d'actions (cf. art. 41 ss ou 97 ss CO)[38].

Si l'employeur viole l'article 328b CO, il engage sa responsabilité contractuelle. C'est notamment le cas lorsque l'employeur traite des données concernant le travailleur qui ne portent pas sur les aptitudes du travailleur à remplir son emploi ou ne sont pas nécessaires à l'exécution du contrat de travail.

L'action en responsabilité contractuelle présente des avantages indéniables pour le demandeur, en ce qui concerne le régime tant du fardeau de la preuve (cf. art. 97 al. 1 CO), de la responsabilité du fait des auxiliaires (cf. art. 101 al. 1 CO) et de la prescription (cf. art. 127 CO)[39].

Il a par exemple été jugé qu'un employeur est tenu de verser des dommages-intérêts à un ancien employé lorsqu'il a fourni de faux renseignements sur son compte, lesquels ont découragé un nouvel employeur de l'embaucher[40].

Au niveau de la ***charge de la preuve***, la preuve de l'atteinte incombe au travailleur, celle d'un éventuel motif justificatif à l'employeur (cf. art. 8 CC)[41].

Une telle charge de la preuve limite la protection effective du travailleur[42]. En effet, le travailleur peut éprouver des difficultés à prouver à la fois l'atteinte à sa personnalité, un dommage, une violation du contrat ou un acte illicite, et le lien de causalité entre la violation ou l'acte illicite et le dommage[43].

---

37 TF 4C.379/2002 du 22 avril 2003, c. 2 ; CAPH/GE du 8 septembre 1992, *in* : JAR 1993, p. 166; BRUNNER/BÜHLER/WAEBER/BRUCHEZ, N 7 *ad* art. 328b CO, p. 157 ; DUNAND, N 114 *ad* art. 328b CO.

38 WERRO, N 1572, p. 441 ; WYLER, Responsabilité, p. 253.

39 DUNAND, N 74 *ad* art. 328 CO.

40 TF 4C.379/2002 du 22 avril 2003, c. 2 ; DUNAND, N 114 *ad* art. 328b CO.

41 MEIER, N 1522, p. 509 ; DUNAND, N 109 *ad* art. 328b CO.

42 DUNAND, N 110 *ad* art. 328b CO.

43 DUNAND, N 110 *ad* art. 328b CO et les références citées.

L'action en réparation du tort moral

Comme l'action en dommages-intérêts, l'action en réparation du tort moral est prévue par l'article 28a CC.

Le travailleur peut obtenir une telle indemnité, fondée sur l'article 49 CO[44], pour autant que les conditions légales posées par cet article soient remplies[45].

L'action en remise du gain

Cette action est mentionnée par l'article 28a CC. Elle paraît devoir rarement s'appliquer en matière de droit du travail.

L'action en réparation du dommage consécutif à une démission avec effet immédiat justifiée

En cas de violation grave de sa personnalité, le travailleur peut également résilier le contrat avec effet immédiat et demander la réparation de son dommage à l'employeur fautif (art. 337b CO)[46].

dd) Les moyens de contre-attaque de l'employeur

Face à des demandes de transmission de données de la part d'un travailleur, l'employeur peut chercher une parade pour refuser cette transmission. Nous avons traité plus haut de la question en ce qui concerne les données personnelles du travailleur[47]. Qu'en est-il lorsque le travailleur ne se borne pas à demander la transmission de ses données personnelles, mais réclame de pouvoir prendre connaissance de données concernant ***d'autres travailleurs*** ? Ce genre de demande interviendra par exemple dans les procès en matière d'égalité salariale entre hommes et femmes ou en matière de versement de bonus ou de primes de départ.

Depuis longtemps, le Tribunal fédéral affirme que l'employeur a l'obligation de répondre à l'injonction du juge lui ordonnant de produire les pièces nécessaires à l'établissement d'une discrimination salariale ou au calcul d'une rémunération variable. L'argument selon lequel la production des pièces par l'employeur faciliterait un éventuel débauchage de

---

44 ArbG/ZH du 10 décembre 2003, *in* : JAR 2004, p. 606 ; BRUNNER/BÜHLER/WAEBER/BRUCHEZ, N 7 *ad* art. 328b CO, p. 157 ; DUNAND, N 114 *ad* art. 328b CO.

45 BRUNNER/BÜHLER/WAEBER/BRUCHEZ, N 7 *ad* art. 328b CO, p. 157 ; DUNAND, N 114 *ad* art. 328b CO.

46 TF, *in* : JAR 1988. 283.

47 Cf. *supra* aa.

certains de ses salariés par des employeurs tiers est inopérant[48]. De plus, le fait pour un salarié de connaître la rémunération des autres salariés d'une entreprise n'est pas un secret d'affaires au sens de l'article 340 alinéa 2 CO[49], ni au sens de l'article 321a alinéa 4 CO[50]. Plus généralement, il n'existe aucune obligation légale pour un salarié de taire le montant de sa rémunération[51].

Dans une affaire récente où le travailleur avait intenté une action en paiement non chiffrée, faute de pouvoir calculer le bonus auquel il prétendait en raison du fait que l'employeur n'avait pas appliqué la méthode de calcul du bonus à laquelle il s'était pourtant contractuellement engagé, le Tribunal fédéral a rappelé que, lorsqu'il intente une action en paiement non chiffrée en faisant valoir qu'il lui manque diverses pièces pour déterminer précisément le bonus auquel il prétend sur une base contractuelle, un travailleur est en droit de demander la production de fiches de salaire et de calcul des bonus d'autres employés, dès lors que l'étude de tels documents lui permettrait de mieux comprendre la manière dont les bonus sont calculés au sein de l'entreprise[52].

Le Tribunal fédéral poursuit en rappelant que la LPD ne s'applique pas aux procédures civiles pendantes (art. 2 al. 2 c LPD) et que les règles spéciales de la procédure assurent déjà suffisamment la protection de la personnalité et il s'agit d'éviter un conflit de norme[53].

En outre, dans le cadre spécifique du calcul d'une rémunération variable, le Tribunal fédéral rappelle que l'article 322a alinéa 2 CO oblige l'employeur à laisser le travailleur consulter ses livres de comptabilité dans la mesure nécessaire. Si l'employeur doit protéger et respecter la personnalité des travailleurs (selon l'art. 328 CO), cette obligation ne fait pas obstacle à la divulgation des revenus de ces derniers. Ainsi, l'employeur ne peut pas refuser de fournir ces données dans le cadre d'une procédure judiciaire entre employeur et travailleur, dans la mesure où le revenu des autres travailleurs au service de l'employeur est pertinent pour le jugement à rendre. La consultation de la comptabilité, garantie par l'article 322a CO au travailleur partie à la procédure, implique même la divulgation de ces informations[54].

Comme autre contre-attaque, l'employeur peut également demander à ce qu'une donnée, même corrigée en faveur du travailleur, soit revêtue de la ***mention de son caractère litigieux***. En effet, le juge peut ordonner la correction d'une donnée – si elle lui apparaît

48 TF 4A_195/2010 du 8 juin 2010, c. 2.3.
49 TF 4A_283/2010 du 11 août 2010, c. 2.3.
50 STREIFF/VON KÄNEL/RUDOLPH, N 2 *ad* art. 322 CO.
51 TF du 14 décembre 1994, *in* : JAR 1995, 214.
52 TF 4A_60/2016 du 10 octobre 2016, c. 2.3 et 3.2.
53 TF 4A_60/2016 du 10 octobre 2016, c. 5.2.2.
54 TF 4A_60/2016 du 10 octobre 2016, c. 5.3 et 5.4.

plus incorrecte que correcte –, tout en assortissant une telle correction de la mention du caractère litigieux de la donnée – s'il conserve tout de même certains doutes sur la vérité de cette donnée[55].

b) Les mesures provisionnelles

Les mesures provisionnelles sont régies par les articles 261 et suivants du CPC.

Concrètement, le travailleur pourrait demander, notamment :

- l'interdiction de la communication de données durant la procédure (cf. art. 262 a CPC) ;
- la rectification provisoire d'une donnée fausse (cf. art. 262 b CPC) ;
- la production de documents ou d'informations nécessaires à la rédaction de l'action à fond[56]. En effet, le Tribunal fédéral a jugé que n'était pas arbitraire la décision d'un juge cantonal d'ordonner à un employeur, par ordonnance de mesures provisionnelles, de communiquer au travailleur, dans les quarante-huit heures dès ordonnance définitive et exécutoire, et sous la commination des peines prévues à l'article 292 CP en cas d'insoumission, des documents tels qu'une convention d'engagement, un contrat de collaboration, un contrat de travail, toutes notes internes à l'employeur concernant le travailleur et portant notamment sur l'appréciation de la qualité de son travail, tout résultat de l'enquête interne en tant qu'il concerne le travailleur, des extraits des procès-verbaux d'organes de l'employeur en tant qu'ils concernent le travailleur, ainsi que les motifs et les circonstances de son licenciement, et les décomptes de rémunération et de salaire[57].

La mesure peut être demandée à titre superprovisionnel si les conditions légales en sont remplies (cf. art. 265 CPC). Un mémoire est également possible (cf. art. 270 CPC).

2. Les actions pénales

Différentes actions pénales existent en matière de protection des données du travailleur. Elles trouvent leur fondement dans la LPD ou dans le CP[58].

---

55 TAF A-4202/2007 du 30 novembre 2007, c. 5.1.2 ; TAF A-5737/2007 du 3 mars 2008, c. 5 ; TAF A-2168/2009 du 21 janvier 2010, c. 5.3.

56 MEIER, N 1829, p. 593 ; cf. également, du même auteur, Le point sur le droit des personnes physiques et le droit de la tutelle, *in* : RSJ 103/2007, p. 467 ; WERMELINGER, N 27 *ad art.* 15 LPD, p. 205. Cf. également DONZALLAZ, N 3888, p. 1418.

57 TF 4P.293/2006 du 9 février 2007.

58 Pour ce dernier, nous renvoyons aux articles 179 et suivants CP.

Sont réprimées :

a) L'inexactitude et l'incomplétude des renseignements fournis, ainsi que la mauvaise exécution du droit d'accès

La personne qui contrevient aux obligations prévues aux articles 8 à 10 et 14 LPD en fournissant, intentionnellement, des renseignements inexacts ou incomplets est punissable, sur plainte, de l'amende (art. 34 al. 1 a LPD).

Selon certains auteurs, serait seul punissable le fait de transmettre au travailleur uniquement certaines données au lieu de transmettre l'ensemble des données ; ne serait pas punissable le refus de transmettre toute donnée[59] ; ainsi, le travailleur qui se verrait refuser catégoriquement par l'employeur tout droit d'accès à son dossier n'aurait que la seule possibilité de réclamer l'exécution de ce droit par une action civile, la condamnation étant susceptible d'être assortie, le cas échéant, de la menace des peines prévues à l'article 292 CP[60].

Cette interprétation de la loi paraît contraire au principe *qui potest majus potest et minus* : en vertu de quelle logique serait-il possible de sanctionner pénalement une transmission de données effectuée, mais de manière incomplète, alors qu'il ne serait pas possible de faire sanctionner une absence totale de transmission ?

Tournons-nous vers l'analyse de la *ratio legis* de cette norme : le Conseil fédéral, dans son message, indique qu'agit de manière pénalement répréhensible le maître du fichier qui ne respecte pas le droit d'accès de la personne concernée[61]. N'est en revanche pas punissable celui qui, invoquant l'article 9 LPD, prétend qu'il n'est pas tenu de fournir de renseignements. Dans ce cas, seule une action de droit civil permet de savoir si le refus ou la restriction du droit d'accès sont justifiés ou non[62]. Le Conseil fédéral précise que la personne qui, contre la vérité, prétend ne détenir aucune information sur la personne concernée tombe sous le coup de cette disposition pénale[63].

L'interprétation de la loi qui nous semble correcte est donc celle-ci : n'est pas punissable pénalement celui a ***une raison manifeste*** de restreindre le droit d'accès, raison dont il devra faire état de manière adéquate. Dans le doute, il convient de ne pas punir pénalement. Toutefois, si l'invocation d'une restriction au droit d'accès apparaît d'emblée comme une

---

59 STREIFF/VON KAENEL/RUDOLPH, N 21 *ad art.* 328b CO.
60 STREIFF/VON KAENEL/RUDOLPH, N 21 *ad art.* 328b CO.
61 Message concernant la LPD, FF 1988 II 443.
62 Message concernant la LPD, FF 1988 II 490.
63 Message concernant la LPD, FF 1988 II 490.

manœuvre dilatoire, une procédure pénale devrait pouvoir être engagée contre le refus d'accorder le droit d'accès.

Une action est « ***intentionnelle*** » au sens de cette disposition lorsque l'employeur connaît le caractère inexact ou incomplet des renseignements qu'il donne. Le Conseil fédéral va plus loin et considère que « commet un dol éventuel, le maître du fichier qui fournit un renseignement, sans aucune vérification, alors même qu'il doute du caractère exact de celui-ci »[64].

b) L'inexécution du devoir d'information lors de la collecte de données

Encourt une amende, la personne qui, intentionnellement, omet d'informer la personne concernée, conformément à l'article 14 alinéa 1 LPD, ou omet de lui fournir les indications prévues à l'article 14 alinéa 2 LPD (art. 34 al. 1 b LPD).

c) La non-déclaration ou la mauvaise déclaration de fichiers au préposé fédéral à la protection des données, ainsi que le refus de collaboration ou la mauvaise collaboration avec ce dernier

Sont punies de l'amende les personnes privées qui, intentionnellement, omettent d'informer le préposé, conformément à l'article 6 alinéa 3 LPD, de déclarer les fichiers visés à l'article 11a LPD ou donnent des indications inexactes lors de leur déclaration (art. 34 al. 2 a LPD) ou qui fournissent au préposé, lors de l'établissement des faits (art. 29 LPD), des renseignements inexacts ou refusent leur collaboration (art. 34 al. 2 b LPD).

d) La violation du devoir de discrétion

La personne qui, intentionnellement, aura révélé d'une manière illicite des données personnelles secrètes et sensibles ou des profils de la personnalité portés à sa connaissance dans l'exercice d'une profession qui requiert la connaissance de telles données, peut être, sur plainte, punie de l'amende (art. 35 al. 1 LPD). Cette disposition devrait pouvoir s'appliquer à tout employeur, quel qu'il soit, vis-à-vis de ses propres salariés[65]. C'est d'ailleurs, du fait de l'exercice de sa propre profession que l'employeur acquiert des données personnelles sur ses employés. Il n'y a pas de raison de mieux protéger les clients d'une société ou les patients d'un psychologue que les travailleurs d'une entreprise à laquelle ils font tout autant confiance lorsqu'ils lui transmettent des informations personnelles qui sont parfois éminemment sensibles.

---

64 Message concernant la LPD, FF 1988 II 490.

65 Du même avis : MEIER, N 2001, pp. 633-634.

Est passible de la même peine la personne qui, intentionnellement, aura révélé d'une manière illicite des données personnelles secrètes et sensibles ou des profils de la personnalité portés à sa connaissance dans le cadre des activités qu'elle exerce pour le compte de la personne soumise à l'obligation de garder le secret ou lors de sa formation chez elle (art. 35 al. 2 LPD).

La révélation illicite de données personnelles secrètes et sensibles, ou de profil de la personnalité, demeure punissable ***alors même que les rapports de travail ou de formation ont pris fin*** (art. 35 al. 3 LPD).

3. Les actions administratives

En parallèle ou indépendamment d'une action civile ou pénale, le travailleur lésé peut ***dénoncer la situation au Préposé à la protection des données***[66]. Ce dernier décidera alors d'ouvrir ou non une enquête administrative. Si le juge civil n'est pas lié par les conclusions auxquelles aboutirait le Préposé, celles-ci pourraient jouer un rôle dans le cadre de la procédure pendante[67].

Il est légalement prévu qu'en présence d'une méthode de traitement susceptible de porter atteinte à la personnalité d'un nombre important de personnes, le Préposé fédéral puisse établir les faits d'office et, le cas échéant, émettre une ***recommandation*** contre le maître de fichier en faute (art. 29 al. 1 a et al. 3 LPD)[68].

Le but d'une telle recommandation est de modifier ou de faire cesser le comportement (art. 29 al. 3 LPD). En soi, la recommandation n'a pas d'effet juridique contraignant. Toutefois, pour autant qu'elle soit acceptée par son destinataire, elle déploie alors un effet direct[69]. En cas de refus, il reste au Préposé la possibilité de porter l'affaire devant le Tribunal administratif fédéral, pour voir la recommandation revêtue de la force obligatoire (art. 29 al. 4 LPD ; art. 35 b LTAF).

Si le préposé constate, à l'issue de l'enquête qu'il a menée en application de ce principe, que la personne concernée risque de subir un préjudice difficilement réparable, il peut requérir des ***mesures provisionnelles*** du président de la cour du Tribunal administratif fédéral compétente en matière de protection des données (art. 33 al. 2 LPD).

Par ailleurs, l'autorité administrative peut ***retirer une autorisation*** qu'elle avait précédemment conférée à une entreprise. Par exemple, une fondation s'est vu retirer

---

66 MEIER, N 1719 et N 1898.

67 MEIER, N 1719 et N 1942.

68 Cf. Préposé fédéral à la protection des données et à la transparence, Guide pour le traitement des données personnelles dans le secteur du travail, octobre 2014, N 2.1.4, p. 5.

69 MEIER, N 1925, p. 618 ; DUNAND, N 120 *ad* art. 328b CO.

l'autorisation de former des apprentis que lui avait accordée la Direction de la formation professionnelle vaudoise, en raison des conditions illégales que la fondation imposait lors de l'engagement d'apprenties[70]. Cette fondation n'embauchait que des personnes de sexe féminin s'engageant notamment à ne pas utiliser de méthode de contraception chimique. Un tel engagement s'accompagnait de demandes de renseignement sur la vie intime des postulantes et des employées.

Le travailleur peut également se fonder sur les voies de droit prévues dans la loi sur le travail (LTr), et notamment son article 59[71].

II. Procédure

Procéduralement, l'action doit être introduite devant une juridiction ***compétente*** (**A**). Elle suivra ensuite l'une des différentes ***sortes de procédures*** (**B**).

A. Compétence

Une action ne sera recevable que si elle est portée devant une juridiction compétente pour en connaître, à la fois ***territorialement*** (**1**) et ***matériellement*** (**2**).

1. La compétence territoriale

Compte tenu de la diversité des systèmes cantonaux d'organisation judiciaire, la compétence territoriale, qui se détermine selon des règles fédérales, doit intervenir en premier lieu lorsqu'il s'agit de déterminer la compétence d'une juridiction. Toutefois, les actions relevant du droit du travail connaissent des fors spéciaux (cf. art. 34 CPC). Il convient dès lors de déterminer si l'action relève du droit du travail ou d'un autre fondement, au sens du CPC.

Selon la doctrine, le travailleur doit pouvoir bénéficier des avantages procéduraux liés au contrat de travail, y compris en matière de protection des données. En effet, le litige relève de la relation de travail et la protection du travailleur est en partie prévue par des

[70] TF 2C_103/2008 du 30 juin 2008.

[71] Cf. Préposé fédéral à la protection des données et à la transparence, Guide pour le traitement des données personnelles dans le secteur du travail, octobre 2014, N 2.1.4, p. 6.

dispositions relevant du contrat de travail (art. 328 et 328b CO)[72]. Pour que les dispositions spéciales de procédure civile s'appliquent, il doit suffire que les prétentions invoquées soient fondées sur des relations de travail de droit privé[73]. Le fondement reste d'ailleurs celui de la protection de la personnalité du travailleur, prise en son aspect spécifique de protection des données personnelles de celui-ci.

La même solution doit prévaloir pour les ***syndicats***. Ces derniers doivent pouvoir agir devant les juridictions du travail lorsqu'ils défendent les intérêts d'un ou de plusieurs travailleurs. Certes, le Tribunal fédéral a jugé que les litiges s'élevant entre un employeur et un organe de contrôle prévu par une convention collective de travail[74], ou entre un employeur et un syndicat défendant des salariés victimes d'un licenciement collectif[75], n'étaient pas des « contestations en matière de droit du travail au sens de l'art. 74 al. 1 let. a LTF ». Si une telle solution devait conduire à refuser, au niveau cantonal, l'accès des syndicats aux juridictions prud'homales, elle serait très certainement critiquable[76].

Pour le ***postulant***, la situation est moins claire. Toutefois, le litige relevant du travail, les juges prud'hommes devraient pouvoir se déclarer compétents.

2. La compétence matérielle

Aux termes des articles 59 alinéa 2 b et 60 CPC, le tribunal doit examiner d'office s'il est compétent à raison de la matière.

Par exemple, dans le canton de Genève, les litiges découlant d'un contrat de travail sont soumis au Tribunal des prud'hommes (art. 1 al. 1 a de la Loi cantonale genevoise sur le Tribunal des prud'hommes). Certes, l'alinéa 2 du même article dispose que les actions en responsabilité dirigées contre les employeurs sur la base de l'article 328 alinéa 2 CO ne sont pas du ressort des prud'hommes. D'aucuns estiment dès lors que les prud'hommes genevois ne seraient compétents pour aucune action en responsabilité de l'employeur pour défaut de protection de la personnalité du travailleur[77]. Il est vrai que le Tribunal de première instance de ce canton s'est déclaré compétent pour connaître d'une action en interdiction de transmission de données de travailleur. Toutefois, ces juges ont – à juste

---

72 AUBERT, Protection, p. 188 ; AUBERT, CR-CO I, N 1 *ad* art. 328b CO, p. 2029 ; BRUNNER/BÜHLER/WAEBER/BRUCHEZ, N 7 *ad* art. 328b CO, p. 157 ; MEIER, N 2061, p. 659 ; DUNAND, N 111 *ad* art. 328b CO.

73 BOHNET/DIETSCHY, N 7 *ad* art. 343 CO.

74 TF 4A_535/2009 du 25 mars 2010, c. 1.2.1 (non publié à l'ATF 137 III 27 = JdT 2011 II 210 = SJ 2011 I 151).

75 TF 4A_449/2010 du 2 décembre 2010, *in* : RSPC 2010, p. 290, c. 1.2.

76 BOHNET/DIETSCHY, N 7 *ad* art. 343 CO ; DIETSCHY, N 13, pp. 11 ss ; cf. WYLER, Note, *in* : RSPC 2011, pp. 102 s.

77 Cf. Guide social romand, fiche « Protection de la personnalité ».

titre selon nous – ajouté que le litige aurait pu être tranché par le Tribunal des prud'hommes : « Pour respecter notamment le principe de l'***unité de la matière*** [nous soulignons], les employés ou les ex-employés [doivent] pouvoir agir, pour toute action civile, qu'elle soit fondée sur la protection des données, le Code civil ou le Code des obligations, par le biais d'une seule demande devant la juridiction du travail lorsque, comme en l'espèce, le litige s'inscrit dans le cadre des rapports de travail[78] ».

Cette position, qui s'autorise de la loi cantonale[79] et de la doctrine[80], nous paraît devoir être suivie.

B. Les sortes de procédures

La LPD dispose que les voies de droit sont régies par les dispositions générales de la procédure fédérale (art. 33 al. 1 LPD).

1. La procédure ordinaire

Selon la jurisprudence, les actions en protection de la personnalité, notamment les actions en interdiction de transmission de données ***ne sont pas de nature patrimoniale***[81], sauf si la demande porte exclusivement sur des dommages-intérêts[82]. Partant, elles doivent suivre la voie de la procédure ordinaire.

En cas de requête de ***mesures provisionnelles par le Préposé fédéral*** auprès du président de la cour du Tribunal administratif fédéral compétente en matière de protection des données, la procédure est régie *a pari* par les articles 79 à 84 de la loi de procédure civile fédérale (art. 33 al. 2 LPD).

2. La procédure simplifiée

Comparée à la procédure ordinaire, la procédure simplifiée se caractérise notamment par un formalisme moindre (art. 244 CPC), une plus grande rapidité et une implication plus forte du juge (art. 247 CPC)[83].

---

78 TPI-GE, JTPI/6136/2015 du 28 mars 2015, c. B.

79 Art. 1 al. 1 a de la Loi genevoise sur le Tribunal des prud'hommes et art. 110 de la loi genevoise sur l'organisation judiciaire.

80 AUBERT, CR-CO I, p. 2029 ; BRUNNER/BÜHLER/WAEBER/BRUCHEZ, p. 153 ; DUNAND, p. 351 ; MEIER, p. 659 ; WYLER/HEINZER, p. 748.

81 TF 4A_328/2015 du 10 février 2016.

82 ATF 127 III 481, c. 1 ; ATF 110 II 411, c. 1; TF 5A_328/2008 du 26 novembre 2008, c. 1 ; CJ-GE ACJC/1529/2015 du 11 décembre 20, c. 1.1 ; JEANDIN, N 12 *ad* art. 308 CPC.

83 ATF 139 III 457, c. 4.4.3.2.

Elle s'applique aux affaires patrimoniales dont la valeur litigieuse ne dépasse pas 30'000 francs (art. 243 al. 1 CPC), ainsi qu'aux actions en exécution du droit d'accès au dossier (art. 15 al. 4 LPD ; art. 243 al. 2 d CPC).

Certaines causes assujetties à la procédure simplifiée bénéficient de la maxime inquisitoire sociale : il s'agit notamment des actions en exécution du droit d'accès, ainsi que des autres litiges portant sur un contrat de travail lorsque la valeur litigieuse ne dépasse pas 30'000 francs (art. 247 al. 2 CPC)[84].

3. Coût de la procédure

Le coût de la procédure se détermine selon les règles applicables aux litiges en matière de droit du travail. La procédure est donc gratuite, de par le droit fédéral, lorsque la valeur litigieuse s'élève jusqu'à 30'000 francs. Les cantons peuvent élever la gratuité à un niveau supérieur, comme c'est le cas par exemple à Genève jusqu'à 75'000 francs (art. 19 al. 3 LaCC/GE).

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.

AUBERT DAVID, Modalités du droit d'accès de l'employé au fichier de son employeur : consultation et obtention de copies des documents transmis à des tiers ; analyse de l'arrêt du Tribunal fédéral 4A_406/2014, *in* : Newsletter droitdutravail.ch, février 2015 (cité : AUBERT, Modalités).

AUBERT GABRIEL, La protection des données dans les rapports de travail, *in* : Gabriel Aubert et al., Journée 1995 de droit du travail et de la sécurité sociale, Zurich 1999, pp. 145-191 (cité : AUBERT, Protection).

AUBERT GABRIEL, Commentaire des art. 319-362 CO, *in* : Luc Thévenoz/Franz Werro (éds.), Commentaire romand, Code des obligations I, 2e édition, Bâle 2012 (cité : AUBERT, CR-CO I).

BOPP LUKAS/BESSENICH BALTHASAR, Kommentar zur Schweizerischen Zivilprozessordnung (ZPO), 3e édition, Zurich/Bâle/Genève 2016.

JEANDIN NICOLAS, Commentaire de l'art. 308 CPC, *in* : François Bohnet et al., CPC – Code de procédure civile commenté, Bâle 2011.

BRÜHWILER JÜRG, Einzelarbeitsvertrag, 3e édition, Bâle 2014.

BRUNNER CHRISTIANE/BÜHLER JEAN-MICHEL/WAEBER JEAN-BERNARD/BRUCHEZ CHRISTIAN, Commentaire du contrat de travail, 3e édition, Lausanne 2004.

[84] TF 4A_636/2015 du 21 juin 2016, c. 2.1.

DIETSCHY PATRICIA, Les conflits de travail en procédure civile suisse, thèse, Neuchâtel/Bâle 2011.

DONATIELLO GIUSEPPE, Droit d'action des organisations au regard de l'art. 89 CPC, *in* : Rémy Wyler (éd.), Panorama II en droit du travail, Berne 2012, pp. 817-835.

DONZALLAZ YVES, Loi sur le Tribunal fédéral – Commentaire, Berne 2008.

DUNAND JEAN-PHILIPPE, Commentaire des art. 328 et 328b CO, *in* : Jean-Philippe Dunand/Pascal Mahon (éds.), Commentaire du contrat de travail, Berne 2013.

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

SCHEIWILLER SARAH, Säumnisfolgen nach der Schweizerischen Zivilprozessordnung, Zurich/Bâle/Genève 2016.

STREIFF ULLIN/VON KAENEL ADRIAN/RUDOLPH ROGER, Arbeitsvertrag – Praxiskommentar zu art. 319-362 OR, 7e édition, Zurich/Bâle/Genève 2012.

THEVENOZ LUC/EMMENEGGER SUSAN/PODA ENDRIT/KISSLING MICHAEL, Le droit bancaire privé suisse 2015, *in* : RSDA 2016, pp. 207-231.

WERMELINGER AMÉDÉO, Commentaire de l'art. 15 LPD, *in* : Bruno Baeriswyl/Kurt Pärli (éds.), Datenschutzgesetz (DSG) - Handkommentar, Berne 2015.

WERRO FRANZ, La responsabilité civile, 2e édition, Berne 2011.

WYLER REMY/HEINZER BORIS, Droit du travail, 3e édition, Berne 2014.

WYLER REMY, La responsabilité civile de l'employeur, y compris en ce qui concerne les actes de ses organes et auxiliaires, *in* : DTA 2011/4, pp. 249-250 (cité : WYLER, Responsabilité).

CAMILLE DUBOIS

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

Sommaire Page

I. Introduction 48

II. Contexte international 48
A. Aperçu des principaux textes applicables 48
B. Développements récents au sein de trois institutions choisies 50
1. Nations Unies 50
2. Conseil de l'Europe 50
3. Union européenne 52
a) Réforme de la législation européenne en matière de protection des données 52
aa) Genèse 52
bb) Règlement (UE) 2016/679 52
cc) Directive (UE) 2016/680 53
b) Transfert de données vers les États-Unis : du « Safe Harbor » au « Privacy Shield » 53

III. Avant-projet de réforme du Conseil fédéral 54
A. Genèse 54
B. Objectifs de la réforme 56
C. Principales nouveautés introduites par l'avant-projet de révision totale de la LPD 57
1. Généralités 57
2. Champ d'application 58
3. Définitions 59
4. Dispositions générales de protection des données 60
a) Principes 60
b) Communication de données personnelles à l'étranger 60
c) Sous-traitance 61
d) Recommandations de bonnes pratiques 61
e) Données personnelles d'une personne décédée 62
5. Obligations des responsables du traitement et des sous-traitants 63
a) Devoir d'information 63
b) Devoirs en cas de décision individuelle automatisée 63
c) Devoir de procéder à une analyse d'impact du traitement 64
d) Devoir de notifier les violations de la protection des données 65
e) Devoir de protéger les données dès la conception et par défaut 66
f) Autres devoirs 67

6. Droits des personnes concernées : droit d'accès 67
7. Spécificités pour le secteur privé 68
a) Atteintes à la personnalité 68
b) Motifs justificatifs 68
c) Prétentions 68
8. Spécificités pour le secteur public 69
a) Bases légales 69
b) Communication de données personnelles 70
c) Prétentions et procédure 70
9. PFPDT 71
10. Dispositions pénales 72
IV. Conclusion 74
Bibliographie 74

I. Introduction

Cette contribution présente l'avant-projet de réforme de la législation fédérale en matière de protection des données, mis en consultation externe par le Conseil fédéral le 21 décembre 2016[1]. Elle s'attache plus particulièrement aux nouveautés introduites par l'avant-projet de révision totale de la loi fédérale sur la protection des données du 19 juin 1992[2], qui constituent le cœur de la réforme, et qui sont susceptibles d'intéresser les différents acteurs du monde du travail.

La réforme proposée par le Conseil fédéral étant intimement liée aux développements en la matière au plan international, il sera préalablement fait un état des lieux à ce niveau.

II. Contexte international

A. Aperçu des principaux textes applicables

La protection des données est garantie sur le plan international par plusieurs textes. Parmi eux la Convention de sauvegarde des droits de l'homme et des libertés fondamentales du 4 novembre 1950[3] (art. 8), la Convention du Conseil de l'Europe du 28 janvier 1981 pour

[1] L'avant-projet, de même que les documents y relatifs, sont disponibles à l'adresse suivante : https://www.bj.admin.ch/bj/fr/home/staat/gesetzgebung/datenschutzstaerkung.html.

[2] LPD, RS 235.1.

[3] Entrée en vigueur pour la Suisse le 28 novembre 1974 (CEDH, RS 0.101).

la protection des personnes à l'égard du traitement automatisé des données à caractère personnel[4] (convention STE 108) et son protocole additionnel du 8 novembre 2001[5], le Pacte international relatif aux droits civils et politiques du 16 décembre 1966[6] (art. 17), ou encore les lignes directrices de l'Organisation de coopération et de développement économiques régissant la protection de la vie privée du 23 septembre 1980, révisées le 11 juin 2013[7].

Dans l'Union européenne (UE), la protection des données trouve ses fondements dans l'art. 16 du Traité sur le fonctionnement de l'Union européenne du 1er janvier 1958[8] et les art. 7 et 8 de la Charte des droits fondamentaux de l'UE du 7 décembre 2000[9]. Sur le plan du droit dérivé, elle est principalement assurée, et ce jusqu'en 2018 (voir ch. II/B/a/aa), par la Directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données[10] (directive 95/46/CE) et par la Décision-cadre 2008/977/JAI du Conseil du 27 novembre 2008 relative à la protection des données à caractère personnel traitées dans le cadre de la coopération policière et judiciaire en matière pénale[11] (décision-cadre 2008/977/JAI). La directive 95/46/CE est notamment complétée, dans le secteur des communications électroniques, par la Directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (Directive e-privacy)[12].

4 Entrée en vigueur pour la Suisse le 1er février 1998 (RS 0.235.1).

5 Entrée en vigueur pour la Suisse le 1er avril 2008 (RS 0.235.11).

6 Entrée en vigueur pour la Suisse le 18 septembre 1992 (RS 0.103.2).

7 Lignes directrices régissant la protection de la vie privée et les flux transfrontières de données de caractère personnel, 1980, consultables à l'adresse : http://www.oecd.org/fr/sti/ieconomie/lignes directricesregissantlaprotectiondelaviepriveeetlesfluxtransfrontieresdedonneesdecaractere personnel.htm ; OECD Guidelines governing the protection of privacy and transborder flows of personal data, 2013, consultables à l'adresse : https://www.oecd.org/sti/ieconomy/2013-oecd-privacy-guidelines.pdf

8 JO C 326 du 26.10.2012, pp. 47 ss.

9 JO C 326 du 26.10.2012, pp. 391 ss.

10 JO L 281 du 23.11.1995, pp. 31 ss.

11 JO L 350 du 30.12.2008, pp. 60 ss.

12 JO L 201 du 31.7.2002, pp. 37 ss. La Commission a publié le 10 janvier dernier une proposition de règlement visant à remplacer cette directive, disponible en ligne sur : https://ec.europa.eu/digital-single-market/en/news/proposal-regulation-privacy-and-electronic-communications.

B. Développements récents au sein de trois institutions choisies

1. Nations Unies

Depuis les révélations d'Edward Snowden en 2013 concernant la surveillance générale d'Internet et des autres moyens de télécommunications par la National Security Agency (NSA), la protection de la sphère privée est devenue un sujet prioritaire pour plusieurs institutions onusiennes.

En 2013, l'Assemblée générale a ainsi adopté une résolution[13], qui invite d'une part les États à réviser leur législation pour garantir le droit au respect de la sphère privée, et d'autre part qui demande au Haut-Commissariat des Nations Unies aux droits de l'homme (HCDH) de rédiger un rapport sur la thématique de la protection de la vie privée en lien avec la surveillance des communications et la collecte de données personnelles. Ce rapport[14] a été livré en 2014. Il conclut notamment que la communication électronique ouvre la voie à une surveillance massive et illimitée et recommande une mobilisation multipartite continue et concertée afin de régler efficacement les problèmes que soulève le droit à la vie privée dans le contexte des technologies de la communication.

Par ailleurs, en 2015, le Conseil des droits de l'homme a décidé de nommer, pour une durée de trois ans, un rapporteur spécial sur le droit à la vie privée. Dans un rapport de mars 2016, constatant certaines carences dans la protection de la sphère privée, le rapporteur a proposé un plan d'action en dix points[15], la première étape étant de développer une définition universelle et détaillée de la notion de sphère privée.

2. Conseil de l'Europe

En 2011, le Conseil de l'Europe a entrepris de moderniser la convention STE 108 et son protocole additionnel, qui datent respectivement de 1981 et de 2001. Un projet de modernisation a été élaboré (P-STE 108)[16]. Le protocole d'amendement y relatif devrait être adopté par le Comité des ministres en 2017.

---

13 Résolution 68/167 du 18 décembre 2013 (http://www.un.org/fr/documents/view_doc.asp?symbol=A/RES/68/167).

14 HCDH, The right to privacy in the digital age, 30 juin 2014 (http://www.humanrights.ch/upload/pdf/141218_Bericht_Pillay.pdf).

15 HCDH, Report of the Special Rapporteur on the right to privacy, 8 mars 2016, ch. 46 ss.

16 Projet consolidé de septembre 2016, disponible en ligne sur : http://www.coe.int/fr/web/data-protection/modernisation-convention108.

Le but de la réforme est principalement d'adapter la convention STE 108 aux nouveaux défis en matière de protection de la sphère privée induits par l'utilisation croissante et généralisée des technologies de l'information et de la communication, à la mondialisation des traitements de données personnelles et aux quantités toujours plus importantes de données traitées[17].

Le projet de modernisation de la convention STE 108 conserve les bases et les principes fondamentaux de l'actuelle convention, tout en renforçant les obligations des responsables du traitement et les droits des personnes concernées. Ainsi, comme aujourd'hui, la future convention ne sera pas d'application directe, couvrira l'ensemble des traitements de données opérés dans le secteur privé et le secteur public, et sera formulée de manière technologiquement neutre afin de pouvoir s'adapter aux évolutions technologiques. Les États parties ne pourront cependant plus formuler de réserve (art. 25).

La convention STE 108, avec son protocole additionnel, constitue à ce jour le seul instrument juridique universel contraignant dans le domaine de la protection des données[18], dans la mesure où elle est ouverte à la ratification d'États non membres du Conseil de l'Europe. À l'heure actuelle, 49 États l'ont ratifiée, dont l'Uruguay, l'Île Maurice et le Sénégal, qui ne sont pas membres du Conseil de l'Europe. Le Cap-Vert, la Tunisie, et le Maroc devraient suivre prochainement. Il est possible que l'intérêt de pays non membres du Conseil de l'Europe pour cette convention STE 108 – respectivement pour le P-STE 108 – grandisse à l'avenir, car la ratification du protocole d'amendement constituera vraisemblablement un critère déterminant pour l'UE pour juger du caractère adéquat des garanties offertes par un pays tiers en cas de communication transfrontière de données (voir les explications sous ch. II/3/b).

---

17 Comité *ad hoc* sur la protection des données, Projet de rapport explicatif – Convention 108 modernisée, 2 juin 2016, ch. 1, disponible en ligne sur : http://www.coe.int/fr/web/data-protection/modernisation-convention108.

18 Le Conseil des ministres a adopté en la matière un grand nombre de recommandations, ayant pour but de préciser la convention. Par exemple : Rec(2010)13 sur 23 novembre 2010 sur la protection des personnes à l'égard du traitement automatisé des données à caractère personnel dans le cadre du profilage ; Rec (2002) 9 du 18 septembre 2002 sur la protection des données à caractère personnel collectées à des fin d'assurance ; Rec (95) 4 du 7 février 1995 sur la protection des données à caractère personnel dans le domaine des services de télécommunication, eu égard notamment aux services téléphoniques ; Rec(89) 2 du 18 janvier 1989 sur la protection des données à caractère personnel utilisées à des fins d'emploi.

3. Union européenne

a) Réforme de la législation européenne en matière de protection des données

aa) Genèse

En 2012, la Commission européenne (la Commission), constatant que l'UE avait besoin d'un cadre juridique plus solide et plus cohérent en matière de protection des données, a décidé de proposer un train de mesures sous la forme d'un paquet comprenant deux actes législatifs : un projet de règlement général sur la protection des données (ci-après : règlement [UE] 2016/679[19]) et un projet de directive relative à la protection des données à caractère personnel traitées à des fins de répression (ci-après : directive [UE] 2016/680[20]).

Ces deux textes ont été adoptés le 27 avril 2016. Le règlement (UE) 2016/679, qui est entré en vigueur le 25 mai 2016, remplacera la directive 95/46/CE à compter du 25 mai 2018 (art. 94 al. 1 règlement [UE] 2016/679), et la directive (UE) 2016/680, qui est entrée en vigueur le 5 mai 2016, remplacera la décision-cadre 2008/977/JAI dès le 6 mai 2018 (art. 59 al. 1 directive [UE] 2016/680).

bb) Règlement (UE) 2016/679

Le règlement (UE) 2016/679, comme la directive 95/46/CE, constituera le texte fondamental en matière de protection des données au niveau de l'UE. A l'instar de celle-ci, il s'appliquera aux traitements de données personnelles de personnes physiques dans le secteur privé et le secteur public. La forme législative choisie, à savoir celle d'un règlement, permettra toutefois de pallier les écarts d'interprétation dans les États membres.

Tout comme le P-STE 108, le règlement (UE) 2016/679 renforce les droits des personnes concernées et les obligations des responsables du traitement. Il contient également une nouvelle disposition sur son champ d'application territorial (art. 3 par. 2), et introduit le principe du guichet unique (art. 56).

---

[19] 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 (JO L 119 du 4.5.2016, pp. 1 ss).

[20] Directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil (JO L 119 du 4.5.2016, pp. 89 ss).

cc) Directive (UE) 2016/680

La directive (UE) 2016/680 s'inspire très largement du règlement (UE) 2016/679. Elle prévoit aussi un renforcement des droits des personnes concernées, et, parallèlement, des obligations supplémentaires pour les responsables du traitement. Elle contient toutefois des règles et des aménagements particuliers propres au domaine pénal. Par ailleurs, compte tenu de sa nature juridique, elle est logiquement beaucoup moins détaillée.

La directive (UE) 2016/680 protège les données personnelles des personnes physiques traitées à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, y compris la protection contre les menaces pour la sécurité publique et la prévention de telles menaces. Elle a pour but d'instituer un niveau élevé de protection tout en facilitant l'échange des données entre les autorités compétentes des différents Etats Schengen.

b) Transfert de données vers les États-Unis : du « Safe Harbor » au « Privacy Shield »

Une affaire qui a fait grand bruit en 2015 est celle de l'annulation[21], par la Cour de Justice de l'UE (CJUE), de la décision de la Commission validant le régime de protection des données mis en place par les États-Unis dans le cadre de l'accord avec l'UE dit « Safe Harbor », ou accord de la « sphère privée » [22]. Cette problématique mérite d'être rapidement présentée ici, dans la mesure où le jugement de la CJUE a eu des répercussions pour la Suisse également.

Selon la directive 95/46/CE, le transfert de données personnelles dans un État non membre de l'UE est subordonné à la condition que ce pays offre un niveau de protection adéquat des données. Ce niveau de protection adéquat peut être constaté par la Commission, dans une décision dite « d'adéquation » (art. 25). Dans ce cas, les données personnelles peuvent être transférées sans autres garanties supplémentaires. En l'absence de décision d'adéquation, le transfert de données vers des pays tiers est subordonné à l'existence de garanties contractuelles ou l'adoption de règles d'entreprises contraignantes (« Binding corporate rules » ou BCR[23]). Ce mécanisme est repris par le règlement (UE) 2016/679 (art. 44ss).

En 2000, l'UE et les États-Unis ont conclu le « Safe Harbor », qui établissait des règles spéciales de protection des données auxquelles les entreprises américaines pouvaient déclarer adhérer. La Commission, par décision du 26 juillet 2000, a constaté que cet

21 Arrêt CJUE C-362/14 *Maximillian Schrems c. Data Protection Commissioner* du 6 octobre 2015.

22 Décision 2000/520/CE du 26 juillet 2000.

23 Il s'agit de codes de conduite internes définissant la politique d'une entreprise en matière de transferts de données personnelles.

accord assurait un niveau de protection adéquat. Les transferts de données personnelles vers les sociétés américaines ayant adhéré au « Safe Harbor » étaient alors automatiquement autorisés.

En 2015, la CJUE, suite à une plainte d'un internaute, qui estimait que, vu les révélations d'Edward Snowden, on ne pouvait plus considérer que le « Safe Harbor » offrait des garanties suffisantes, a annulé la décision d'adéquation de la Commission. Elle a constaté que la Commission n'avait pas examiné que les États-Unis assuraient effectivement, par leur législation, leurs engagements internationaux, mais qu'elle s'était contentée d'analyser le régime du « Safe Harbor ». La CJUE a jugé principalement qu'aucune règle n'empêchait l'État américain d'avoir un accès illimité aux données personnelles des ressortissants de l'UE.

Suite à ce jugement, l'UE et les États-Unis ont négocié un nouveau cadre pour le transfert de données aux entreprises américaines : le « Privacy Shield » ou « bouclier de protection des données ». La décision d'adéquation y relative de la Commission a été adoptée le 12 juillet 2016. Le « Privacy Shield » est entré en vigueur le 1er août 2016[24].

La Suisse avait conclu en 2008 avec les États-Unis un accord comparable à l'ancien « Safe Harbor », le « U.S.-Swiss Safe Harbor Framework ». Suite à l'arrêt de la CJUE, le régime pour le transfert des données personnelles depuis la Suisse à des entreprises sises aux États-Unis a été renégocié. Le Conseil fédéral a pris acte de ce nouveau régime le 11 janvier dernier. La nouvelle réglementation correspond désormais à la solution en vigueur entre les États-Unis et les pays membres de l'UE et de l'Espace économique européen[25].

III. Avant-projet de réforme du Conseil fédéral

A. Genèse

La réforme a été historiquement déclenchée par une évaluation de la LPD, commandée par l'Office fédéral de la justice (OFJ) en 2010[26]. Compte tenu des évolutions technologiques intervenues depuis l'entrée en vigueur de la loi en 1993 et de l'art. 170 de la Constitution

[24] JO C 2016 du 1.8.2016.

[25] Voir le communiqué de presse du Conseil fédéral : https://www.admin.ch/gov/fr/accueil/documentation/communiques.msg-id-65210.html.

[26] BOLLIGER/FÉRAUD/EPINEY/HÄNNI.

fédérale[27], la Confédération se devait en effet d'examiner si la LPD était encore adaptée aux réalités. L'évaluation s'est concentrée sur certains aspects particuliers de la loi, à savoir sa notoriété, ainsi que sur ses mécanismes de mise en œuvre. Par ailleurs, il n'a pas été tenu compte des nouveautés introduites par les révisions de 2008[28] et 2010[29], faute de disposer du recul nécessaire.

Il est ressorti de l'évaluation que la LPD a permis d'atteindre un bon niveau de protection s'agissant des problèmes déjà connus à l'époque, mais que les développements technologiques et la modification des comportements sociaux correspondante ont fait émerger de nouveaux dangers pour la protection des données auxquels la loi ne peut plus faire face. Ces derniers découlent principalement de l'augmentation du volume de données traitées, du manque de transparence des traitements – qui empêche les personnes concernées de faire valoir leurs droits et le Préposé fédéral à la protection des données et à la transparence (PFPDT) d'exercer sa surveillance – de l'internationalisation des traitements – qui rend difficile la mise en œuvre des droits des personnes concernées –, et enfin, de la perte de contrôle sur les données personnelles découlant de l'utilisation croissante d'Internet[30].

Sur la base de ce constat, le Conseil fédéral a chargé le Département fédéral de justice et police (DFJP) – à l'interne l'OFJ – d'examiner quelles mesures pouvaient améliorer la protection des données, en tenant compte des réformes en cours au niveau européen, encore peu avancées alors. Les mesures en question devaient permettre de renforcer la protection des données plus en amont, d'améliorer la transparence des traitements et la maîtrise des personnes concernées sur leurs données, d'en améliorer le contrôle et enfin de protéger plus efficacement les mineurs et de mieux sensibiliser le public[31]. Un groupe de travail – composé de représentants de l'administration fédérale, des cantons, des milieux économiques, des associations de protection des consommateurs ainsi que d'experts – a dans ce but été constitué. Ses réflexions ont été consignées dans une esquisse d'acte normatif[32], qui a plus à voir avec un rapport compte tenu de sa longueur et de sa densité. Le Conseil fédéral en a pris connaissance le 1er avril 2015 et sur sa base a chargé le DFJP d'élaborer, en collaboration avec d'autres départements[33], un avant-projet de

27 Cst., RS 101.

28 RO 2008 4983.

29 RO 2010 3387.

30 Rapport du Conseil fédéral du 9 décembre 2011 sur l'évaluation de la loi fédérale sur la protection des données, FF 2012 255.

31 Rapport du Conseil fédéral du 9 décembre 2011 sur l'évaluation de la loi fédérale sur la protection des données, FF 2012 255 (268).

32 Esquisse d'acte normatif relative à la révision de la loi sur la protection des données du Groupe d'accompagnement Révision, 29 octobre 2014.

33 Le PFPDT, le Département fédéral de l'économie, de la formation et de la recherche (DEFR), le Département fédéral des finances (DFF) et le Département fédéral de l'intérieur (DFI).

réforme. Ce dernier est en procédure de consultation externe depuis le 21 décembre 2016, et jusqu'au 4 avril 2017.

L'avant-projet se présente sous la forme d'un acte modificateur unique dénommé « Avant-projet de loi fédérale sur la révision totale de la loi sur la protection des données et sur la modification d'autres lois fédérales » (ci-après : AP). Le chiffre I de cet acte comprend la révision totale de la LPD (ci-après : AP-LPD) et, en annexe, les modifications d'autres lois fédérales rendues nécessaires par la révision cette loi. Le chiffre II comprend la modification des lois fédérales exigées par la reprise de la directive (UE) 2016/680 (voir *infra* B).

B. Objectifs de la réforme

La réforme vise à renforcer la législation fédérale en matière de protections des données pour l'adapter aux nouvelles technologies. Il s'agit notamment d'améliorer la transparence des traitements, d'améliorer la maîtrise des personnes concernées sur leurs données personnelles, et d'améliorer le contrôle, par les autorités, des traitements de données. Elle vise dans le même temps à préserver l'économie, en créant un environnement législatif encourageant l'innovation – en lien avec la société numérique notamment – ainsi que les flux transfrontières de données.

Parallèlement la réforme doit tenir compte de certains développements au niveau européen.

Tout d'abord, elle doit rendre la législation suisse compatible avec le P-STE 108, afin de pouvoir, le moment venu, ratifier le protocole d'amendement sans révision législative complémentaire. Le Conseil fédéral estime que la ratification par la Suisse de ce protocole est nécessaire, tant pour des motifs tenant à la protection des droits de l'homme que pour des raisons économiques. Concernant ce second point, il considère que la ratification du protocole d'amendement sera un critère déterminant pour la Commission lorsqu'elle aura à décider du maintien de la décision d'adéquation dont bénéficie la Suisse pour le transfert de données personnelles avec l'UE[34].

Ensuite, la réforme doit intégrer les exigences de la directive (UE) 2016/680, dans la mesure où celle-ci constitue un développement de l'acquis de Schengen, que la Suisse s'est engagée à reprendre[35]. La directive (UE) 2016/680 n'est pas directement applicable et doit être transposée. En tant qu'État associé, la Suisse pourrait en principe se contenter

[34] Rapport explicatif concernant l'avant-projet de loi fédérale sur la révision totale de la loi sur la protection des données et sur la modification d'autres lois fédérales du 21 décembre 2016, p. 29.

[35] Art. 2 par. 3 de l'Accord entre la Confédération suisse, l'Union européenne et la Communauté européenne sur l'association de la Confédération suisse à la mise en œuvre, à l'application et au développement de l'acquis de Schengen du 26 octobre 2004 (RS 0.362.31).

de transposer les exigences de la directive pour les traitements s'inscrivant dans le cadre de la coopération instaurée par Schengen dans le domaine pénal. Toutefois, étant donné que le contenu de la directive (UE) 2016/680 rejoint en grande partie celui du P-STE 108 le Conseil fédéral a décidé de la reprendre plus largement. Ainsi, ses dispositions sont tantôt intégrées dans l'AP-LPD (chiffre I de l'AP), tantôt, lorsqu'il s'agit de règles propres au domaine de la coopération pénale, dans les législations spécifiques (soit dans le chiffre II de l'AP).

Finalement, l'avant-projet doit permettre un rapprochement de la législation suisse avec le règlement (UE) 679/2016. Ce dernier ne constitue pas un développement de l'acquis de Schengen et ne lie donc en principe pas la Suisse. Il est toutefois important pour le transfert de données avec l'UE. En effet, comme mentionné sous ch. II/B/3/b, l'échange de données entre l'UE et un pays tiers ne peut se faire que si ce pays tiers assure un niveau de protection adéquat, niveau de protection qui peut être constaté par la Commission dans une décision d'adéquation. La Suisse est actuellement au bénéfice d'une telle décision[36]. Cette dernière se fonde toutefois sur le niveau de protection défini par la directive 95/46/CE. Or, à l'avenir, l'examen de la législation suisse se fera à l'aune du règlement (UE) 2016/679. Ainsi, si la Suisse souhaite conserver la décision d'adéquation dont elle bénéficie, elle doit rapprocher sa législation des exigences de ce texte.

C. Principales nouveautés introduites par l'avant-projet de révision totale de la LPD

1. Généralités

Les changements intéressant le secteur du travail sont contenus dans l'avant-projet de révision totale de la LPD. La contribution se limitera dès lors à présenter les principales innovations pertinentes de ce texte. Les modifications des lois spéciales en matière de coopération pénale liées à la reprise de la directive (UE) 2016/680 ne seront en particulier pas abordées. La présentation suivra la systématique de l'AP-LPD.

La révision ne modifie pas la relation entre la législation générale en matière de protection des données et les lois spéciales. L'AP-LPD s'appliquera donc, sous réserve de dispositions particulières, aux employeurs privés et aux employeurs publics fédéraux dans la même mesure que l'actuelle LPD. La structure générale de la loi n'est pas non plus fondamentalement modifiée. Ainsi, après une partie générale applicable au secteur privé et au secteur public (sections 1 à 4), l'AP-LPD contient une section dédiée aux traitements

[36] Décision de la Commission du 26 juillet 2000 relative à la constatation, conformément à la directive 95/46/CE du Parlement européen et du Conseil, du caractère adéquat de la protection des données à caractère personnel en Suisse, JO L 215 du 25.8.2000, p. 1.

de données par des personnes privées (section 5), une section dédiée aux traitements de données par des organes fédéraux (section 6), une section consacrée au PFPDT (section 7), une aux dispositions pénales (section 8) et une section avec les dispositions finales (section 10). La section 9 contient une disposition sur la conclusion de traités internationaux, qui figure aujourd'hui dans les dispositions finales (art. 36 al. 5 LPD).

La contribution recourt à dessein à une terminologie neutre, évitant d'assimiler l'employeur au responsable du traitement et l'employé à la personne dont les données sont traitées. En effet, l'employé peut aussi être selon les cas lui-même responsable du traitement, par exemple lorsqu'il collecte des données sur son employeur, ou sur des collègues. Par ailleurs, le monde du travail ne se limite pas à ces deux catégories de personnes, mais compte d'autres acteurs, tels des assureurs privés ou publics, des agences de location de placement, ou encore des services cantonaux (en matière d'emploi, d'impôt, ou d'état civil), aussi potentiellements concernés par l'AP-LPD. Enfin, pour des raisons de lisibilité et d'espace, les explications qui suivent ne mentionnent en principe pas, pour chaque nouveauté présentée, si elle est exigée par le P-STE 108, la directive (UE) 2016/680 ou le règlement (UE) 2016/679. Le lecteur consultera le rapport explicatif du Conseil fédéral concernant l'avant-projet de loi fédérale sur la révision totale de la loi sur la protection des données et sur la modification d'autres lois fédérales du 21 décembre 2016 (rapport explicatif). Bien souvent ceci dit, les mesures importantes sont prévues par les trois textes.

2. Champ d'application

L'AP-LPD prévoit quelques modifications concernant le champ d'application de la loi. Ainsi, notamment, la future LPD ne devrait plus s'appliquer aux traitements de données concernant des personnes morales (art. 2 al. 1 AP-LPD). Cette modification part du constat que la protection actuelle n'a pas, ou peu de portée pratique, ce qui nuit à l'efficience de loi[37]. La protection offerte par d'autres textes législatifs, tels que le Code civil[38] (art. 28ss), la loi fédérale du 19 décembre 1986 sur la concurrence déloyale[39], la loi fédérale du 9 octobre 1992 sur le droit d'auteur[40], les règles sur les secrets professionnels, d'affaires et de fabrication est, selon le Conseil fédéral, suffisante. Il est à noter qu'une telle protection n'est prévue ni par les textes de l'UE ni par le P-STE 108, ni encore par la nette majorité des législations étrangères. Son abrogation permettra ainsi certainement de favoriser les flux transfrontières, dans la mesure où les données concernant des personnes

37 Sur cette thématique, voir DRECHSLER, pp. 85-86.
38 CC, RS 210.
39 LCD, RS 241.
40 LDA, RS 231.1.

morales pourront à l'avenir être transférées à l'étranger sans qu'un niveau de protection adéquat soit requis (art. 5 et 6 AP-LPD).

3. Définitions

L'avant-projet prévoit de rapprocher la terminologie de la LPD des textes européens.

Ainsi, par exemple, la notion de « maître du fichier » est remplacée par celle de « responsable du traitement », et la définition de « sous-traitant » introduite. Par ailleurs, la liste exhaustive des données sensibles est élargie aux données génétiques (art. 3 let. c ch. 3 AP-LPD) et aux données biométriques identifiant une personne de façon unique, telles que les images faciales ou les empreintes digitales (art. 3 let. c ch. 4 AP-LPD).

L'AP-LPD supprime la notion de « profil de la personnalité », qui est une spécificité suisse et qui n'existe ni en droit européen, ni dans les législations étrangères. Le Conseil fédéral estime que cette institution est dépassée par les évolutions technologiques, et que la protection spéciale que lui confère la LPD a peu d'effets en pratique. Il propose de la remplacer, par la notion de « profilage », aussi prévue par les textes UE (art. 3 par. 4 de la directive [UE] 2016/680 et art. 4 par. 4 du règlement [UE] 2016/679).

Selon l'AP-LPD (art. 3 let. f), le profilage est l'exploitation, automatisée ou non, de données personnelles ou non, consistant à analyser ou prédire les caractéristiques essentielles d'une personne, telles que son rendement au travail, sa situation économique, sa santé, sa sphère intime ou ses déplacements. Le profilage est largement utilisé pour procéder à de la publicité ciblée, ou dans le domaine bancaire, pour évaluer les risques des clients futurs ou présents. La définition de l'avant-projet englobe l'exploitation de données non personnelles, afin de tenir compte du fait qu'avec les technologies actuelles l'exploitation de données sans lien avec une personne fait souvent émerger des données personnelles[41], ou que les données exploitées pour prédire les caractéristiques d'une personne déterminée sont aussi souvent des données anonymisées. Le rattachement avec la LPD se fait par l'analyse et la prédiction des caractéristiques essentielles d'une personne, qui constituent-elles des données personnelles[42].

Enfin, l'AP-LPD supprime la notion de fichier, pour tenir compte des nouvelles réalités. En effet, d'une part, vu les avancées en informatique, tout ou presque constitue aujourd'hui un fichier. D'autre part, certaines activités susceptibles d'avoir d'importantes conséquences pour les personnes concernées, telles que le profilage, ne conduisent pas forcément à la création d'un fichier, ou alors seulement d'un fichier éphémère. Elles

41 Selon une étude américaine, jusqu'à 87% des personnes résidants aux États-Unis pourraient être identifiées uniquement à partir de trois données en soit anonymes : le code postal, la date de naissance et le sexe (SWEENEY), p. 16.

42 Rapport explicatif, p. 43.

échappent ainsi actuellement aux dispositions de la loi impliquant l'existence d'un fichier (art. 8 ou 14 LPD par exemple), ce qui n'est pas satisfaisant.

4. Dispositions générales de protection des données

a) Principes

La plupart des modifications concernant les principes sont d'ordre rédactionnel et systématique.

L'AP-LPD renforce toutefois les exigences relatives au consentement (art. 4 al. 6 AP-LPD). À l'avenir, lorsque le consentement sera nécessaire pour justifier un traitement de données, il devra, en plus d'être libre et éclairé, être clair. Un consentement ne pourra ainsi plus être déduit du silence ou de l'inaction de la personne concernée. Il sera en revanche toujours possible d'admettre un consentement par actes concluants, pour autant que les exigences de clarté soient remplies (une personne conclut un contrat, qui entraîne nécessairement le traitement de certaines données personnelles). S'agissant du consentement pour les données sensibles et le profilage, l'AP-LPD prévoit qu'il doit être exprès. Cela permet notamment de supprimer la controverse doctrinale actuelle s'agissant de la qualité du consentement de l'art. 4 al. 5 LPD[43]. Le consentement exprès doit résulter d'une déclaration écrite ou orale ou de signes. Cette condition est remplie en cochant une case, ou en cliquant sur un bouton « suivant » par exemple[44].

b) Communication de données personnelles à l'étranger

L'avant-projet réaménage les règles actuelles en la matière (art. 6 LPD), sans toutefois modifier singulièrement les conditions auxquelles des données peuvent être communiquées à l'étranger.

Il reprend tout d'abord le principe de base qui veut qu'aucune donnée ne puisse être transmise à l'étranger si la personnalité de la personne concernée devait s'en trouver gravement menacée (art. 5 al. 1 AP-LP).

Il prévoit ensuite un système en cascade :

– un transfert de données à l'étranger sera tout d'abord possible si le Conseil fédéral a constaté, par voie d'ordonnance, que l'État concerné dispose d'une législation assurant

[43] Certains auteurs estiment que le consentement explicite de l'art. 4 al. 5 LPD exclut un consentement donné par actes concluants, et d'autres non, pour autant que l'intention de la personne concernée soit claire. Pour un résumé des avis sur cette question voir : VASELLA.

[44] Pour plus de détails voir Rapport explicatif, p. 46.

un niveau de protection adéquat (art. 5 al. 2 AP-LPD). Cette ordonnance remplacera la liste actuellement établie par le PFPDT[45].

– en l'absence d'une telle ordonnance, un transfert sera possible si d'autres garanties assurent un niveau de protection approprié dans l'État en question (art. 5 al. 3 AP-LPD). Ces garanties pourront résulter de différents instruments : traité international, garanties spécifiques ou standardisées contractuelles, règles d'entreprises contraignantes (art. 5 let. a à d AP-LPD, qui reprend pour l'essentiel les garanties de l'actuel art. 6 al. 2 let. a et g LPD). Ce qui est nouveau c'est que le PFPDT sera chargé à l'avenir d'approuver ou d'établir certaines de ces garanties (art. 5 al. 4 à 6 AP-LPD).
– en l'absence de niveau de protection adéquat ou approprié, des données pourront exceptionnellement être transférées, à certaines conditions. L'AP-LPD reprend dans les grandes lignes le catalogue de l'actuel art. 6 al. 2 let. b à f LPD. Deux nouveaux cas de figure sont prévus : les données sont contenues dans un registre public destiné à informer le public, le transfert est nécessaire pour protéger la vie ou l'intégrité corporelle d'un tiers[46].

c) Sous-traitance

L'art. 7 AP-LPD introduit une nouveauté significative concernant la sous-traitance. Dorénavant, le sous-traitant qui entend lui-même sous-traiter un traitement à un tiers ne pourra le faire qu'avec l'accord écrit préalable du responsable du traitement. Cet accord pourra être donné de manière générale. Dans ce cas toutefois, le sous-traitant devra informer le responsable du traitement de tout changement (ajout ou remplacement d'autres sous-traitants), afin que ce dernier puisse le cas échéant s'opposer à ces changements.

Parallèlement, l'AP-LPD prévoit que le responsable du traitement devra informer la personne concernée lorsqu'il confie un traitement à un sous-traitant, et lui communiquer les données ou catégories de données personnelles concernées (art. 13 al. 4 AP-LPD).

d) Recommandations de bonnes pratiques

L'un des objectifs de la révision est de responsabiliser les personnes concernées, qui doivent être sensibilisées aux risques pour la protection des données et être en mesure d'adapter leurs comportements, mais aussi les responsables du traitement et les sous-traitants, qui doivent être encouragés à adopter spontanément des conduites respectueuses de la protection des données.

---

45 Consultable à l'adresse suivante : https://www.edoeb.admin.ch/datenschutz/00626/00753/index.html?lang=fr.

46 Pour plus de détails voir Rapport explicatif, pp. 46-50.

Le Conseil fédéral propose, à l'égard des responsables du traitement et des sous-traitants, de formaliser l'édiction de recommandations de bonnes pratiques, pour les secteurs privé et public (art. 8 AP-LPD). Les recommandations seront élaborées par le PFPDT ou par les milieux concernés, qui pourront les soumettre pour approbation à ce dernier. L'idée est ici véritablement de favoriser l'autorégulation, et la prise de décisions concertées puisque même dans le cas où elles émaneront du PFPDT, les recommandations devront être élaborées avec le concours des milieux intéressés.

Ces recommandations auront principalement pour but de concrétiser la loi. Elles permettront de préciser certaines notions, et les modalités de certains droits et devoirs. Elles permettront aussi de disposer de solutions et de standards plus détaillés dans des secteurs particuliers (vidéosurveillance, Cloud-computing, réseaux sociaux).

Le PFPDT publiera les recommandations qu'il a approuvées ou édictées (art. 8 al. 3 AP-LPD). Elles ne seront pas obligatoires, et les dispositions de protection des données pourront être respectées d'une autre manière[47].

e) Données personnelles d'une personne décédée

L'art. 12 AP-LPD régit l'accès aux données d'une personne décédée – actuellement partiellement réglé à l'art. 1 al. 7 de l'ordonnance du 14 juin 1993 relative à la loi fédérale sur la protection des données[48] – et leur effacement.

L'avant-projet prévoit d'une part que les personnes disposant d'un intérêt légitime pourront consulter gratuitement les données personnelles d'une personne décédée, sauf si le défunt l'a expressément interdit de son vivant ou en cas d'intérêt prépondérant contraire de ce dernier ou d'un tiers. L'intérêt légitime sera présumé en cas de lien de parenté directe avec le défunt, de mariage, de partenariat enregistré ou de concubinage au moment du décès. Le responsable du traitement ne pourra invoquer aucun secret de fonction ou professionnel.

D'autre part, l'AP-LPD prévoit que chaque héritier pourra demander l'effacement ou la destruction de ces données, à moins que le défunt l'ait expressément interdit de son vivant ou en cas d'intérêt prépondérant contraire de ce dernier ou d'un tiers. Ce droit sera expressément réservé à chaque héritier, individuellement, et sera indépendant de tout traitement illicite de données. La disposition permettra par là d'assurer, à certaines conditions, la « mort numérique » des personnes décédées. Il sera ainsi en pratique plus facile de faire effacer un compte d'utilisateur sur un réseau social, ou une messagerie.

---

47 Pour plus de détails voir Rapport explicatif, pp. 50-52.

48 OLPD, RS 235.11.

Les actions en exécution de l'art. 12 AP-LPD seront soumises, comme les actions en exécution du droit d'accès, à la procédure simplifiée de l'art. 243 du Code de procédure civile du 19 décembre 2008[49] (annexe à l'AP-LPD, ch. 11)[50].

5. Obligations des responsables du traitement et des sous-traitants

a) Devoir d'information

Le devoir d'information est un élément central pour garantir la transparence des traitements et le contrôle des personnes concernées sur leurs données personnelles. Il est en effet impossible de faire valoir ses droits sans savoir que des données personnelles sont collectées. L'AP-LPD renforce la législation sur deux points principalement.

Premièrement, le devoir d'information ne sera plus limité, dans le secteur privé, à la collecte de données sensibles (art. 14 LPD). Comme c'est le cas actuellement déjà dans le secteur public (art. 18 LPD), il vaudra pour tous les types de données personnelles (art. 13 al. 1 AP-LPD). Par ailleurs, en plus de l'identité et des coordonnées du responsable du traitement, des données ou catégories de données traitées (nouveau), des finalités du traitement ainsi que des destinataires ou des catégories de destinataires éventuels, la personne concernée devra être informée de toutes les informations nécessaires à la mise en oeuvre de ses droits et garantissant la transparence du traitement. L'étendue de ces informations variera selon le type de données personnelles traitées (sensibles ou non par exemple) ainsi que, notamment de la nature et de l'ampleur du traitement. La formulation large de la disposition permettra d'adopter des recommandations de bonnes pratiques différenciées, tenant compte des besoins spécifiques aux différents secteurs concernés.

Deuxièmement, l'AP-LPD prévoit que le responsable du traitement, en cas de sous-traitance, communique à la personne concernée l'identité et les coordonnées du sous-traitant ainsi les données ou catégories de données personnelles traitées (art. 13 al. 4 AP-LPD)[51].

b) Devoirs en cas de décision individuelle automatisée

L'AP-LPD contient une disposition spéciale s'agissant des décisions individuelles automatisées, de plus en plus fréquentes dans tous les secteurs de l'économie, mais aussi dans le secteur public (art. 15 AP-LPD).

---

49 CPC, RS 272.

50 Pour plus de détails sur cette disposition voir Rapport explicatif, pp. 52 et 53.

51 Pour plus de détails sur ce point voir Rapport explicatif, pp. 54-56.

D'une part, le responsable du traitement devra informer la personne concernée de l'existence d'une décision individuelle automatisée lorsque cette dernière a des effets juridiques pour elle ou l'affecte de manière significative. D'autre part, il devra lui donner la possibilité de faire valoir son point de vue, sur la décision en tant que telle, ainsi que sur les données traitées. Ces devoirs tomberont lorsque la décision individuelle automatisée est prévue par la loi.

Il y a une décision individuelle automatisée lorsqu'un traitement de données a lieu sans intervention humaine, et qu'il en résulte une décision, respectivement un jugement ou une évaluation à l'égard de la personne concernée. Peu importe que la décision soit communiquée par une personne physique, dans la mesure où cette dernière n'a pas d'influence sur le processus de décision. De telles décisions sont fréquentes. On peut par exemple citer les cas dans lesquels la conclusion d'un contrat dépend d'un bilan de la situation financière automatisé de la personne concernée, ou de l'évaluation automatisée de ses données de santé par un algorithme. Dans le secteur public, constituent de telles décisions par exemple les amendes en matière de circulation routière, qui sont envoyées automatiquement au conducteur sur la base d'une prise de vue, ou encore les décisions de taxation automatisées.

Ces décisions sont problématiques sous l'angle de la transparence. En effet, la personne concernée ne connaît pas les motifs qui ont conduit à la décision, et ne peut influer sur son contenu, alors qu'il est des cas dans lesquels les éléments pris en compte sont faux, obsolètes, ou méritent une interprétation différente de celle qu'en fait une machine. Les problèmes surviennent particulièrement lorsque la décision a des effets négatifs pour la personne concernée, par exemple lorsqu'on lui refuse la conclusion d'un contrat parce qu'elle a été qualifiée d'insolvable par erreur. L'AP-LPD garantit que la personne concernée n'est pas soumise à une décision prise sans intervention humaine[52].

c) Devoir de procéder à une analyse d'impact du traitement

L'AP-LPD suit une approche fondée sur le risque. Il prévoit des solutions différenciées selon les risques potentiels pour les droits des personnes concernées que représente un traitement. Ces risques dépendent largement des activités menées par les responsables du traitement et par les sous-traitants. Ainsi, les activités présentant un risque accru seront soumises à des règles plus strictes que celles présentant un risque moindre.

Une mesure qui traduit bien cette approche est celle de l'analyse d'impact du traitement. En vertu de l'art. 16 al. 1 LPD, une telle analyse devra être menée lorsque le traitement envisagé est susceptible d'entraîner un risque accru pour les droits de la personne

[52] Pour plus de détails sur ce point voir Rapport explicatif, pp. 56 et 57.

concernée. L'analyse permettra anticiper d'éventuels problèmes et d'éviter les coûts qui pourraient en résulter.

Pratiquement, il s'agira dans un premier temps de faire un pronostic des conséquences possibles du traitement pour la personne concernée. Le risque accru pourra par exemple découler de la nature des données traitées (données sensibles par ex.), de la nature et du but du traitement (profilage par ex.), de la quantité de données traitées, de leur transmission dans d'autres pays (en l'absence d'une protection appropriée par ex.) ou du fait qu'elles sont accessibles à un plus ou moins grand nombre de personnes.

Si le responsable du traitement ou le sous-traitant arrive à la conclusion que le traitement envisagé présente un risque accru, il procèdera à l'analyse. Celle-ci devra exposer le traitement envisagé, notamment les différents processus, le but du traitement et la durée de conservation des données, et expliquer quels risques le traitement implique. Il s'agira ici de reprendre et d'approfondir l'estimation qui aura été faite en amont, lors de l'examen de la nécessité de procéder à une étude d'impact. L'étude d'impact devra enfin expliquer par quelles mesures les risques sont réduits. Cela passera souvent de mettre en œuvre les principes de l'art. 4 AP-LPD, ainsi que les principes de protection dès la conception et par défaut (privacy by design/by default ; art. 18 AP-LPD). Il faudra faire une pesée des intérêts entre ceux de la personne concernée et ceux du responsable du traitement ou du sous-traitant. Cette balance devra être intégrée à l'étude d'impact du traitement et motivée en conséquence.

L'analyse sera ensuite communiquée au PFPDT, qui devra faire par des ses éventuelles objections dans un délai de trois mois à compter de la réception de toutes les informations nécessaires (art. 16 al. 3 et 4 AP-LPD)[53].

d) Devoir de notifier les violations de la protection des données

Bien souvent, les cas de vol, de destruction ou de perte de données personnelles restent confidentiels. Peu nombreuses en effet sont les entreprises qui, spontanément, rendent public un piratage de leurs serveurs ou la destruction accidentelle de données. Or de telles situations se produisent de plus en plus fréquemment[54].

L'art. 17 al. 1 AP-LPD prévoit une ainsi obligation pour le responsable du traitement de notifier sans délai tout traitement non autorisé ou toute perte de données au PFPDT. L'obligation tombe si situation ne présente vraisemblablement pas de risques pour la

---

53 Pour plus de détails sur cette mesure voir Rapport explicatif, pp. 57-59.

54 Pour s'en convaincre, on pourra consulter le site Internet suivant, qui répertorie les plus grands cas de violations de sécurité de l'accès aux données dans le monde de la dernière décennie : http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/?utm_source=datafloq&utm_medium=ref&utm_campaign=datafloq.

personne concernée. La notification permettra au PFPDT de prendre le cas échéant des mesures à l'égard du responsable du traitement afin de rétablir la situation et de prévenir de nouveaux cas.

En cas de demande du PFPDT, ou si les circonstances le requièrent, la personne concernée devra aussi être informée (art. 17 al. 2 AP-LPD). Tel est le cas si l'information est susceptible de réduire les risques pour la personne concernée, par exemple parce qu'elle lui permet de prendre les mesures nécessaires pour se protéger (modification d'un mot de passe par ex.). Cette communication pourra être restreinte, différée ou supprimée dans les cas prévus à l'art. 14 al. 3 et 4 AP-LPD (art. 17 al. 3 AP-LPD).

Le sous-traitant devra pour sa part uniquement informer le responsable du traitement, qui appréciera si une notification au PFPDT et/ou à la personne concernée est nécessaire (art. 17 al. 4 AP-LPD)[55].

e) Devoir de protéger les données dès la conception et par défaut

La réforme introduit l'obligation, pour les responsables du traitement et les sous-traitants, d'observer les principes de privacy by design (protection des données dès la conception) et de privacy by default (protection des données par défaut).

Le premier principe impose de prendre dès la conception du traitement les mesures appropriées permettant de prévenir et de minimiser les atteintes aux droits des personnes concernées. Cela passe par la mise en place d'un ensemble de mesures techniques et organisationnelles conformes aux principes définis à l'art. 4 AP-LPD. Il est par exemple possible d'enregistrer des échéances régulières dans un système informatique pour que les données personnelles qui ne sont plus nécessaires aux finalités du traitement soient effacées ou anonymisées automatiquement (respect des principes de proportionnalité et de finalité).

Le second principe commande de prendre des mesures pour garantir que, par défaut, seules sont traitées les données nécessaires à la finalité du traitement. Le responsable du traitement ou le sous-traitant prédéfinit par exemple certains réglages respectueux de la protection des données, qui s'appliquent par défaut lorsque la personne ne choisit pas une autre option.

Le lien entre les deux principes est étroit, car les réglages prédéfinis s'inscrivent souvent dans un système entier respectueux de la protection des données.[56].

---

[55] Pour plus de détails sur cette mesure voir Rapport explicatif, pp. 59 et 60.

[56] Sur ces questions voir Rapport explicatif, pp. 60-61.

f) Autres devoirs

L'AP-LPD prévoit encore deux autres obligations pour le responsable du traitement et le sous-traitant.

L'art. 19 al. 1 AP-LPD introduit un devoir de documenter les traitements de données personnelles. Cette disposition remplace l'obligation faite aux privés de faire enregistrer leurs fichiers par le PFPDT, qui est bureaucratique et par ailleurs peu utile, dans la mesure où la LPD prévoit plusieurs exceptions à l'obligation d'enregistrement (art. 11a LPD). Le devoir de documenter le traitement des données s'appliquera à tous les processus de traitement des données. Son contenu sera précisé par voie d'ordonnance.

L'art. 19 al. 2 AP-LPD prévoit quant à lui que le responsable du traitement et le sous-traitant informent les destinataires de toute rectification, effacement, destruction ou violation de la protection des données et de toute limitation du traitement selon l'art. 25 al. 2 ou 34 al. 2 AP-LPD. Cette disposition permettra d'éviter que des tiers qui n'auraient pas connaissance de ces modifications continuent de traiter illicitement des données personnelles. Il pourra être renoncé à la communication si elle est impossible ou exige des efforts disproportionnés, ce qu'il ne faudra admettre qu'avec retenue.

6. Droits des personnes concernées : droit d'accès

Le catalogue des informations à fournir à la personne concernée en cas d'exercice du droit d'accès est élargi (art. 20 al. 2 AP-LPD). Celle-ci doit recevoir toutes les informations nécessaires pour qu'elle puisse faire valoir ses droits et pour que la transparence soit garantie. Il s'agit dans tous les cas de l'identité et des coordonnées du responsable du traitement, des données traitées, de la finalité du traitement, de la durée de la conservation des données ou, si cela n'est pas possible, des critères pour la fixer, de l'existence d'une décision individuelle automatisée, des informations disponibles sur l'origine des données, ainsi que des informations prévues à l'art. 13 al. 3 et 4 AP-LPD.

L'al. 3 prévoit encore que si une décision à l'égard de la personne concernée est prise, des informations supplémentaires sur le résultat de cette décision, la manière dont elle a été prise ainsi que sur les conséquences et sa portée doivent être communiquées à la personne concernée. Ces informations supplémentaires seront surtout utiles en cas de décisions individuelles automatisées. La personne devra pouvoir comprendre sur quelles bases la décision a été prise et quelles sont les conséquences pour elle, ce qui implique que le responsable du traitement lui communique quelle importance les données traitées ont eu sur la décision.

Les motifs et les modalités permettant de restreindre le droit d'accès seront pour l'essentiel les mêmes qu'actuellement (art. 9 LPD)[57].

7. Spécificités pour le secteur privé

a) Atteintes à la personnalité

L'article 23 AP-LPD correspond pour l'essentiel à l'art. 12 LPD.

L'AP-LPD introduit une nouvelle fiction d'atteinte : le fait de procéder à du profilage sans le consentement exprès de la personne concernée.

b) Motifs justificatifs

L'art. 24 AP-LPD reprend en substance l'art. 13 LPD en listant les motifs permettant de supprimer l'illicéité de l'atteinte. La réforme implique deux nouveautés.

Premièrement, s'agissant du motif tiré de l'évaluation du crédit de la personne concernée (al. 2 let. c), l'AP-LPD prévoit qu'il ne pourra à l'avenir entrer en ligne de compte que si – en plus des conditions actuelles – la personne concernée est majeure. Malgré la capacité de contracter limitée des personnes mineures, on remarque en effet des abus dans ce domaine. Les conditions sont renforcées également s'agissant des traitements opérés à des fins ne se rapportant pas à des personnes (al. 2 let. e). Ce motif justificatif n'entrera en ligne de compte que si les données personnelles sont rendues anonymes dès que le but du traitement le permet (al. 2 let. e ch. 1), et si, s'agissant de données sensibles, elles sont communiquées à des tiers uniquement sous une forme ne permettant pas d'identifier la personne concernée (al. 2 let. e ch. 2). Cette mesure tient compte des possibilités offertes par le Big Data et de l'augmentation du nombre de traitements de données sensibles.

c) Prétentions

L'art. 25 al. 1 AP-LPD reprend sur le principe l'art. 15 al. 1 LPD en le complétant.

L'avant-projet mentionne expressément le droit à l'effacement. Cet ajout est symbolique, dans la mesure où ce droit existe déjà en application de la législation actuelle, par le renvoi de l'art. 15 LPD à l'art. 28 CC[58]. Il permet cependant de faire écho à l'arrêt « Google

[57] Pour plus de détails voir Rapport explicatif, pp. 62-64.

[58] Le droit à l'effacement correspond dans le domaine de la protection des données au « droit à l'oubli », tel que conféré de manière générale par la protection de la personnalité du droit civil (ATF 109 II 353 ; ATF 111 II 209 et ATF 122 II 449).

Spain » de la CJUE[59] et de mieux renseigner les personnes concernées sur l'étendue de leurs droits.

L'art. 25 al. 2 AP-LPD prévoit une nouveauté : lorsque ni l'exactitude ni l'inexactitude d'une donnée personnelle ne peut être établie, le demandeur pourra demander, outre la mention du caractère litigieux, la limitation du traitement. Cela signifie que les données en question seront marquées de façon à ce que leur utilisation soit limitée à ce qui est nécessaire pour constater leur exactitude ou leur inexactitude. Le marquage pourra consister à déplacer temporairement les données dans un autre système de traitement, à rendre les données inaccessibles aux utilisateurs, ou à retirer temporairement les données publiées d'un site internet.

La réforme prévoit aussi, s'agissant des actions en justice, des modifications relatives aux frais judiciaires en procédure civile. L'évaluation de la LPD a montré que les personnes concernées font rarement valoir leurs droits, principalement dans le secteur privé, notamment en raison de craintes concernant les coûts d'un procès[60]. Cela nuit à l'efficacité de la loi. Cette situation a par ailleurs empêché le développement d'une jurisprudence différenciée, concrétisant les normes et garantissant une certaine sécurité juridique. Pour faciliter l'accès des personnes concernées à la justice, l'AP-LPD prévoit ainsi de supprimer les frais de justice pour les actions civiles en matière de protection des données. L'art. 99 CPC est ainsi modifié de sorte que les actions et requêtes fondées sur la LPD soient exemptes de l'obligation de fournir des sûretés, l'art. 113 CPC est complété de manière à ce que, pour les procédures de conciliation menées en application de la LPD, il ne soit pas perçu de frais judiciaires, et l'art. 114 CPC est complété de façon à ce que, dans la procédure au fond, il ne soit pas perçu de frais judiciaires pour les litiges relevant de la LPD (voir l'annexe à l'AP-LPD, ch. 11)[61].

8. Spécificités pour le secteur public

a) Bases légales

L'art. 27 LPD reprend dans les grandes lignes l'art. 17 LPD en le reformulant. Il reproduit tout d'abord l'exigence de base légale formelle, en l'étendant au profilage. Il énumère ensuite les cas dans lesquels une base légale matérielle suffit et introduit une condition supplémentaire : que le traitement ne soit pas susceptible d'entraîner des risques particuliers pour les droits des personnes concernées (al. 2 let. b). L'al. 3 mentionne

---

59 Affaire CJUE C-131/12 *Google Spain SL et Google Inc. contre Agencia Española de Protección de Datos (AEPD) et Mario Costeja González* du 13 mai 2014.

60 BOLLIGER/FÉRAUD/EPINEY/HÄNNI, pp. 90 ss et 219.

61 Pour plus de détails sur les art. 23 à 25 AP-LPD voir Rapport explicatif, pp. 64-67.

ensuite les cas dans lesquels aucune base légale n'est nécessaire. Il reprend les actuelles let. b et c de l'art. 17 LPD et ajoute un cas de figure : si le traitement est nécessaire pour protéger la vie et l'intégrité corporelle de la personne concernée ou d'un tiers et qu'il n'est pas possible d'obtenir le consentement de la personne concernée dans un délai raisonnable (let. c)[62].

b) Communication de données personnelles

L'art. 29 AP-LPD reprend le principe de l'art. 19 LPD, selon lequel les organes fédéraux ne peuvent communiquer des données personnelles que s'il existe une base légale, et précise qu'il s'agit d'une base légale selon l'art. 27 al. 1 et 2 AP-LPD (actuellement le renvoi est fait à l'art. 17 al. 1 LPD). La disposition ne renvoie ainsi plus aux exceptions prévues par l'art. 27 AP-LPD (resp. 17 LPD). Les cas dans lesquels les organes fédéraux sont habilités à communiquer des données personnelles en l'absence d'une base légale sont énumérés de manière exhaustive à l'art. 29 al. 2 let. a à e AP-LPD. Cette reformulation permet de mettre fin à l'actuelle controverse sur la portée des exceptions de l'art. 19 al. 1 let. a à d LPD[63]. Le catalogue des exceptions est par ailleurs élargi. Ainsi, un organe fédéral pourra communiquer des données dans un cas d'espèce non seulement lorsque ces dernières sont indispensables au destinataire pour l'accomplissement d'une tâche légale mais aussi lorsque cela est indispensable pour l'organe fédéral qui envisage de communiquer les données. Par ailleurs, il pourra aussi le faire si cela est nécessaire pour protéger la vie et l'intégrité corporelle de la personne concernée ou d'un tiers et qu'il n'est pas possible d'obtenir le consentement de la personne concernée dans un délai raisonnable comme à l'art. 27 al. 3 let. c AP-LPD.

Enfin, l'exigence de base légale formelle pour les procédures d'appel, soit les données accessibles en ligne, dans des systèmes d'information, est abandonnée. Cette exigence, en plus d'être dépassée à l'heure où tout ou presque est informatisé, rompt avec le caractère technologiquement neutre de la loi[64].

c) Prétentions et procédure

Les prétentions et la procédure selon la nouvelle loi correspondent largement à ce que prévoit la LPD. Trois nouveautés significatives sont à mentionner.

---

62 Pour plus de détails voir Rapport explicatif, p. 68.

63 La question est de savoir si les exceptions visent aussi la communication de données sensibles et de profils de la personnalité, ou si cette dernière est régie par l'art. 17 al. 2 LPD, le catalogue n'étant pas tout à fait identique. Pour un résumé des avis sur cette problématique, voir EHRENSPERGER, N 22 ss *ad* art. 19 LPD.

64 Pour plus de détails voir Rapport explicatif, p. 69.

Tout d'abord, l'art. 34 al. 2 AP-LPD introduit un devoir, pour l'organe fédéral, de limiter le traitement des données lorsque leur exactitude ou leur inexactitude ne peut être un prouvée (voir *supra* III/D/7/c).

Ensuite, pour les mêmes raisons qu'à l'art. 25 AP-LPD, l'avant-projet mentionne ici aussi expressément la possibilité d'exiger l'effacement des données.

Enfin, l'art. 34 al. 4 AP-LPD prévoit une règle particulière s'agissant des prétentions à l'égard des institutions patrimoniales publiques : la rectification, l'effacement ou la destruction des données ne pourra être exigée d'elles s'agissant des fonds qu'elles gèrent. Cette disposition vise des institutions publiques telles que les Archives fédérales, qui ont comme activité de collecter des documents, de les exploiter et de les rendre accessibles. Une rectification, un effacement ou une destruction de données personnelles irait à l'encontre d'une telle activité, pour autant que cette mesure porte sur les fonds archivistiques de ces institutions. En effet, ces fonds doivent en quelque sorte photographier un moment du passé, ce qui n'est possible que si les documents qu'ils contiennent sont conservés dans leur forme originale. Il en va de l'intérêt public à la liberté d'information (art. 16 al. 3 Cst.). La seconde phrase de l'al. 4 permet toutefois à la personne d'exiger, pour autant qu'elle dispose d'un intérêt prépondérant, une limitation de l'accès aux données litigieuses. Cette exception tient compte de la tendance toujours plus grande de publier des archives publiques sur Internet[65].

9. PFPDT

La nouveauté la plus significative introduite pas l'avant-projet s'agissant du PFPDT concerne ses compétences. Alors qu'actuellement il ne peut émettre que des recommandations (art. 27 et 29 LPD), il a été décidé de lui conférer à l'avenir le pouvoir de rendre des décisions contraignantes. Ces nouveaux pouvoirs sont prévus par le P-STE 108, la directive (UE) 2016/680 et le règlement (UE) 2016/679.

Le PFPDT pourra à l'avenir mener des procédures d'enquête, d'office ou sur dénonciation, contre un privé ou un organe fédéral si des indices font penser qu'un traitement viole des dispositions de protection des données. Le dénonciateur n'aura pas qualité de partie à la procédure, mais s'il s'agit de la personne concernée le PFPDT devra l'informer de la suite donnée à sa dénonciation. Le PFPDT disposera d'une certaine marge de manœuvre s'agissant de l'ouverture ou non d'une enquête (art. 41 AP-LPD).

Dans le cadre de son enquête le PFPDT pourra ordonner certaines mesures d'investigation (inspection sans préavis des locaux et accès à toutes les données et informations nécessaires) si la personne privée ou l'organe fédéral ne respecte pas son obligation de collaborer et si toutes les tentatives pour obtenir les renseignements et les documents

[65] Pour plus de détails voir Rapport explicatif, pp. 70 et 71.

nécessaires sont restées vaines. Il pourra aussi prononcer des mesures provisoires, qu'il pourra faire exécuter avec l'aide d'autres autorités fédérales ou des organes de police cantonaux et communaux (art. 42 AP-LPD). Dans tous les cas il est prévu qu'il puisse vérifier en dehors de toute enquête si une personne privée ou un organe fédéral respecte les dispositions fédérales de protection des données. Cela lui permettra de conserver une partie de l'activité informelle nécessaire dont il jouit aujourd'hui (art. 41 al. 4 AP-LPD).

En cas de violation de la loi, le PFPDT pourra ordonner la suspension, la cessation, ou la modification des traitements. Cela concerne aussi les communications à l'étranger (art. 43 AP-LPD). Il ne pourra en revanche pas prononcer d'amendes administratives.

La procédure applicable sera la loi fédérale du 20 décembre 1967 sur la procédure administrative[66]. Seul pourra recourir l'organe fédéral ou la personne privée contre qui les mesures auront été prises. Le PFPDT pourra recourir contre les décisions prises sur recours du Tribunal administratif fédéral (art. 44 AP-LPD).

L'art. 45 AP-LPD prévoit une obligation pour le préposer de dénoncer aux autorités pénales compétentes les infractions dont il a connaissance dans l'exercice de ses fonctions[67].

10. Dispositions pénales

Le Conseil fédéral a fait le choix de ne pas conférer au PFPDT le pouvoir d'infliger des amendes administratives. Il aurait fallu pour ce faire selon toute vraisemblance modifier entièrement l'organisation du PFPDT, de façon à en faire une autorité collégiale, sur le modèle de la Commission fédérale de la concurrence par exemple. Cela aurait engendré des frais considérables. Le Conseil fédéral estime au surplus préférable de prononcer des sanctions dans le cadre de procédures pénales. Par ailleurs, l'organisation actuelle du PFPDT fonctionne plutôt bien. Elle permet des interventions rapides et est peu bureaucratique. L'option choisie s'inscrit à contre-courant des législations étrangères, et implique un renforcement significatif du volet pénal de la loi, pour satisfaire au P-STE 108, qui prévoit que les sanctions doivent être dissuasives, mais aussi en regard de la décision d'adéquation de la Commission.

L'avant-projet prévoit ainsi notamment d'augmenter pour toutes les contraventions la limite maximale des amendes que pourront prononcer les autorités de poursuite pénales cantonales à 500'000 francs.

L'art. 50 AP-LPD reprend sur le principe l'actuel art. 34 LPD en le complétant pour tenir compte notamment des nouvelles obligations incombant aux responsables du traitement et

66 PA, RS 172.021.

67 Pour plus de détails sur le PFPDT voir Rapport explicatif, pp. 72-78.

aux sous-traitants, et en étendant la punissabilité à la négligence. Parmi les nouvelles dispositions dont la violation sera punissable, signalons l'art. 15 (devoir d'informer en cas de décision individuelle automatisée), l'art. 16 (communication de l'étude d'impact du traitement au PFPDT), l'art. 17 (devoir de notification des violations de la protection des données), et l'art. 19 let. b (devoir d'informer les destinataires de toute rectification, effacement, destruction, violation de la protection des données ainsi que toute limitation du traitement). Par ailleurs le fait de ne pas se conformer à une décision du PFPDT sera également punissable.

L'art. 51 AP-LPD est nouveau. Il découle notamment du fait que l'avant-projet contient toute une série de nouvelles obligations pour les responsables du traitement et les sous-traitants. Il ne s'appliquera, comme l'article précédent – et comme l'art. 34 LPD – qu'aux personnes privées. Seront punissables, sur plainte, les comportements suivants : confier le traitement de données à un sous-traitant en violation de l'art. 7 al. 1 et 2 AP-LPD, ne pas prendre les mesures nécessaires pour protéger les données contre tout traitement non autorisé et toute perte (art. 11 AP-LPD), ne pas procéder à une étude d'impact en violation de l'art. 16 AP-LPD, ne pas prendre les mesures appropriées au sens de l'art. 18 AP-LPD et le fait de ne pas documenter les traitements de données conformément à l'art. 19 let. a AP-LPD. Ici aussi, la négligence sera punissable.

L'art. 52 AP-LPD reprend l'art. 35 LPD concernant la violation du devoir de discrétion en le renforçant. Premièrement, le devoir de discrétion ne concernera pas uniquement les données sensibles, mais toutes les données, pour autant qu'elles soient secrètes. Deuxièmement, l'état de fait punissable est étendu à la révélation de données traitées à des fins commerciales. Cette adaptation permet de tenir compte des développements technologiques, qui ont notamment eu pour conséquence de fortement faciliter le traitement de données sensibles et le profilage à des fins purement lucratives, par des commerçants ou des réseaux sociaux par exemple. Enfin, l'AP-LPD prévoit désormais un délit passible d'une peine privative de liberté de trois ans au plus ou d'une peine pécuniaire au lieu d'une amende.

L'avant-projet prévoit une disposition facilitant quelque peu la poursuite des entreprises, qui ne sont actuellement pas punissables puisque l'art. 102 du Code pénal[68] ne s'applique pas aux contraventions. Il reprend la réglementation prévue à l'art. 7 de la loi du 22 mars 1974 sur le droit pénal administratif[69], en relevant à 100'000 francs le montant maximal de l'amende au-delà duquel il n'est plus possible de poursuivre la personne morale en lieu et place des personnes physiques.

---

68 CP, RS 311.0.

69 DPA, RS 313.0.

Enfin, le délai de prescription de l'action pénale, à la base de 3 ans (art. 109 CP), est élevé à 5 ans, afin que les enquêtes, souvent compliquées et fastidieuses en matière de protection des données, ne soient pas vaines[70].

IV. Conclusion

En renforçant sa législation, la Suisse remplit ses obligations internationales, et devrait pouvoir assurer la libre circulation des données avec l'UE. La réforme aura aussi pour effet indirect de renforcer la confiance des consommateurs s'agissant du traitement de leurs données personnelles. De ce point de vue, la réforme est susceptible engendrer des retombées positives non seulement pour les consommateurs, mais aussi pour les entreprises, qui pourront développer de nouvelles opportunités d'affaires, dans le domaine du commerce électronique, ou du stockage de données par exemple. Les coûts nécessaires au respect des nouvelles obligations[71] - qui dépendront en pratique largement des modalités de mise en œuvre – devraient ainsi être compensés, notamment, par les avantages découlant du libre transfert des données avec l'UE et le développement de nouvelles perspectives d'activités.

La LPD est et restera une loi générale, à caractère transversal, et technologiquement neutre. Ce n'est qu'à ces conditions qu'elle pourra survivre aux évolutions technologiques. Les problématiques liées à des secteurs particuliers devront, comme c'est le cas aujourd'hui, être précisées par des lois spéciales, ou plus souplement, par des recommandations de bonnes pratiques. Des mesures plus ciblées pourraient d'ailleurs découler d'autres travaux menés actuellement au plan fédéral, tels que le Programme national de recherche 75 « Big Data »[72], les travaux du Groupe d'experts « Avenir du traitement et de la sécurité des données », ou encore le Programme « Jeunes et médias - protection des enfants et des jeunes face aux médias numériques »[73].

Bibliographie

BOLLIGER CHRISTIAN/FÉRAUD MARIUS/EPINEY ASTRID/HÄNNI JULIA, Evaluation des Bundesgesetzes über den Datenschutz – Schlussbericht, Berne 10 mars 2011.

70 Pour plus de détails sur les dispositions pénales voir Rapport explicatif, pp. 79-82.

71 Les conséquences pour l'économie ont fait l'objet d'une analyse d'impact de la réglementation : PRICEWATERHOUSECOOPERS AG.

72 http://www.nfp75.ch/fr/Pages/Home.aspx.

73 Pour plus d'indications sur ces travaux voir Rapport explicatif, p. 10.

DRECHSLER CHRISTIAN, Plädoyer für die Abschaffung des Datenschutzes für juristische Personen, *in* : PJA 2016, pp. 80 ss.

EHRENSPERGER JENNIFER, Commentaire de l'art. 19 LPD, *in* : Urs Maurer-Lambrou/Gabor-Paul Blechta (éds.), Datenschutzgesetz/Öffentlichkeitsgesetz – Basler Kommentar, 3e édition, Bâle 2014, N 22 ss.

PRICEWATERHOUSECOOPERS AG, Regulierungsfolgenabschätzung (RFA) zur Revision des eidg. Datenschutzgesetzes (DSG), 11 juin 2016.

SWEENEY LATANYA, Uniqueness of Simple Demographics in the U.S. Population, Carnegie Mellon University, School of Computer Science, Data Privacy Laboratory, Technical Report LIDAP-WP4, Pittsburgh 2000, disponible en ligne sur : http://dataprivacylab.org/projects/identifiability/paper1.pdf.

VASELLA DAVID, Zur Freiwilligkeit und zur Ausdrücklichkeit der Einwilligung im Datenschutzrecht, *in* : Jusletter 16 novembre 2015.

JEAN-PHILIPPE WALTER*

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

Sommaire

		Page
I.	Introduction	78
II.	Loi fédérale sur la transparence	79
	A. Objet	79
	B. Champ d'application	80
	C. Notion de document officiel	82
	1. Autres documents	83
	2. Document à l'usage personnel	83
	D. Droit d'accès à un document officiel	84
	1. Limitation de l'accès à un document officiel	85
	2. Accès à des données personnelles	87
	a) Notion de données personnelles	88
	b) Anonymisation des données	89
	aa) Limite au devoir d'anonymisation	91
	c) Vie privée contre intérêt public	92
	aa) Accomplissement d'une tâche publique	93
	bb) Intérêt public prépondérant	94
	d) Atteinte à la vie privée	95
	aa) Intensité de l'atteinte	97
	e) Accès à ses propres données et à celles de tiers	97
	E. Jurisprudence concernant l'accès aux données des employés de la Confédération	99
	1. Communication d'une liste de collaborateurs traitant des dossiers de la Comco	99
	2. Accès à l'agenda Outlook d'un haut fonctionnaire	100
	3. Demande d'accès à la liste des activités accessoires des employés fédéraux	101
	4. Demande d'accès aux résultats d'une enquête administrative	102
	F. Droit d'être entendu	103
III.	Conclusion	105
Bibliographie		106

* Je remercie Marc Moinat pour la relecture du texte et l'établissement de la documentation nécessaire à cette contribution.

I. Introduction

L'information et la communication constituent deux caractéristiques essentielles de la société actuelle. Si par le passé, le culte du secret et le règne de la non-transparence ont dominé nos sociétés, elles deviennent aujourd'hui plus ouvertes tout en garantissant aux individus le droit au respect de leur vie privée. Le principe de l'accès à l'information et aux documents officiels, ainsi que le droit à la protection des données sont dès lors deux impératifs démocratiques, nécessaires au fonctionnement d'une société de l'information proche des citoyens. À l'instar de nombreux pays européens, il souffle en Suisse également un vent de transparence. Comme la majorité des cantons, la Confédération a adopté une loi fédérale sur la transparence dans l'administration (loi sur la transparence, LTrans) qui est entrée en vigueur le 1er juillet 2006[1]. L'introduction du principe de la transparence dans l'administration entraîne progressivement un changement de culture administrative. Jusqu'alors, la règle du secret a prédominé et l'accès à l'information était l'exception. Avec ce changement de paradigme, il revient à l'administration de justifier la non-communication d'un document. Ce pourra être le cas lorsqu'un document contient des données personnelles et que leur divulgation porterait atteinte à la sphère privée des personnes concernées sans être justifié par un intérêt public prépondérant, comme nous le verrons par après.

Ainsi d'un côté l'administration se doit d'être transparente et de l'autre elle se doit de respecter le droit à la vie privée garanti par l'article 8 CEDH et l'article 13 de la Constitution et concrétisé dans la loi fédérale et les 26 lois cantonales sur la protection des données. Le défi est donc de concilier l'intérêt à la transparence et le droit à la protection des données et à la vie privée. Même si selon le message du Conseil fédéral, « la protection des données personnelles […] prime par principe le droit à l'accès »[2], il n'y a pas lieu de faire prévaloir plutôt une loi par rapport à l'autre. Le principe de transparence est à considérer comme un intérêt public supérieur ou significatif qui découle des principes ancrés dans la Constitution, de l'État de droit et de la démocratie[3]. Il doit être concilié avec le droit à la protection des données et à la vie privée qui constitue également un des éléments essentiels d'une société démocratique garantissant le respect et l'exercice des droits et libertés fondamentales.

1 RS 152.3.
2 FF 2003 1857.
3 AMMANN/LANG, p. 917 et auteurs cités.

II. Loi fédérale sur la transparence

A. Objet

L'objectif est de promouvoir la transparence sur les activités de l'administration. Aux termes de l'article 1 LTrans, le but et l'objet de la loi sont la promotion de « la transparence quant à la mission, l'organisation et l'activité de l'administration ». L'information est également une ressource publique qu'il convient de partager. La loi donne ainsi un droit de regard aux citoyens et citoyennes sur le fonctionnement de l'État et contribue ainsi à l'information du public en garantissant l'accès aux informations contenues dans des documents officiels[4]. Elle les invite à s'impliquer davantage dans les affaires publiques. Le principe de transparence doit permettre en particulier un contrôle démocratique des activités des autorités et des administrations publiques et est un élément de la confiance des citoyens et citoyennes dans le fonctionnement de leurs institutions. Ce droit d'accès peut se fonder partiellement sur l'article 16 Cst. « liberté d'information »[5] et est un élément du contrôle démocratique qui permet de rééquilibrer les relations entre les administrations et leurs administrés. Comme cela ressort du message du Conseil fédéral relatif à la LTrans[6], le principe de transparence doit contribuer à concrétiser le droit à l'information de l'article 16 alinéa 3 Cst., renforcer les droits démocratiques et le contrôle direct de l'administration par les citoyens et contribuer à rendre l'administration plus proche des préoccupations de la société. Il doit permettre de diminuer les indiscrétions et rendre l'administration plus efficace et plus effective.

La loi règle cependant uniquement l'information passive. Elle n'oblige pas l'administration à publier des informations de manière active. Toutefois, l'article 21 LTrans donne la compétence au Conseil fédéral d'édicter des dispositions concernant l'information sur les documents officiels et leur publication. Il a fait usage de cette compétence dans l'ordonnance d'application[7] en prévoyant que les autorités publient sur internet des informations sur les domaines et les affaires importantes relevant de leur compétence et mettent à disposition des intéressés toutes informations susceptibles de faciliter la recherche de documents officiels. En outre les autorités compétentes doivent publier sur internet les documents officiels importants pour autant que cela ne contrevienne pas à des dispositions légales[8].

---

4 BRUNNER, N 12 *ad* art. 1 LTrans.

5 BRUNNER, N 3 *ad* art. 1 LTrans.

6 FF 2003 1817.

7 Art. 18 de l'ordonnance du 24 mai 2006 sur le principe de la transparence dans l'administration (OTrans, RS 152.31).

8 Art.19 OTrans.

B. Champ d'application

Le champ d'application est défini en raison de la personne et en raison de la matière. Ainsi selon l'article 2, la loi s'applique à l'administration fédérale et aux organismes de droit public ou de droit privé extérieurs à l'administration, dans la mesure où ils édictent des actes ou rendent en première instance des décisions, ainsi qu'aux services du Parlement. Elle ne s'applique par contre pas à la Banque Nationale suisse et à l'Autorité fédérale de surveillance des marchés financiers. Le Conseil fédéral peut soustraire de l'application de la LTrans d'autres entités si l'accomplissement de leurs tâches l'exige, s'il y a un risque d'atteinte à leur capacité de concurrence ou leurs tâches sont d'importance mineure[9]. Cette délégation de compétence qui me parait juridiquement contestable[10] n'a à ce jour pas été utilisée par le Conseil fédéral. Selon le message, ces « exceptions pourraient se révéler nécessaires notamment dans les domaines dans lesquels les tâches confiées à des unités décentralisées consistent presque exclusivement dans le traitement de données personnelles ou de données devant être classées dans la catégorie des secrets professionnels ou des secrets d'affaires »[11]. Relevons que les exceptions prévues dans la loi notamment à l'article 7 alinéa 1 lettre g et 7 alinéa 2 permettent de tenir suffisamment compte de ces situations.

En raison de la matière, la loi ne s'applique pas à l'accès aux documents officiels concernant les procédures civiles, pénales, d'entraide judiciaire et administrative internationale, de règlement international des différends, aux procédures juridictionnelles de droit public, y compris administratives, ainsi qu'aux procédures d'arbitrages[12]. Ces exceptions se justifient pour éviter une concurrence de normes entre les dispositions de la LTrans et les dispositions spécifiques de procédure qui régissent l'accès aux documents[13]. Cette exception couvre les procédures pendantes. La question de savoir si elle couvre également les procédures closes n'a pas été définitivement tranchée par la justice. Toutefois, avec la doctrine dominante, j'estime que les exceptions de l'article 3 lettre a LTrans ne couvrent que les documents faisant partie d'une procédure pendante[14]. Une exclusion générale du champ d'application matérielle de la LTrans des documents officiels d'une procédure close aurait pour conséquence d'exclure à jamais du principe de transparence des documents qui ont été élaborés par exemple dans le cadre d'une

9 Art. 2 al. 3 let. a à c LTrans.

10 Du même avis, SÄGESSER, N 60 *ad* art. 2 LTrans.

11 FF 2003 1831.

12 Art. 3 al. 1 let. a LTrans.

13 TAF A-8073/2015 du 13 juillet 2016, c. 5.2.1.

14 SCHWEIZER/WIDMER, N 12 *ad* art. 3 LTrans ; BRUNNER, N 19 *ad* art. 26 PA ; AMMANN/LANG, N 25.22.

procédure de première instance ou qui avaient été produits par ou remis à l'administration avant toute procédure au sens de l'article 3 alinéa 1 lettre a LTrans. De cette manière, il serait possible par l'entremise de l'ouverture d'une procédure, de créer des domaines secrets de l'activité administrative, ce qui irait à l'encontre de l'objectif de la loi. Seuls échappent à l'accès selon la LTrans, les documents qui ont été élaborés explicitement pour l'ouverture d'une procédure ou dans le cadre de la procédure (recours, échange d'écriture, etc.). L'accès à ces documents est régi par les dispositions spéciales du droit de procédure[15].

La loi ne s'applique également pas à la consultation du dossier par une partie dans une procédure administrative de première instance[16]. Ce sont les règles de la procédure administrative qui s'appliquent. La loi ne s'appliquera en outre plus aux documents officiels portant sur la recherche d'informations au sens de la loi fédérale du 25 septembre 2015 sur le renseignement[17]. Je relève malheureusement que des pressions s'exercent de la part de certaines administrations pour obtenir du législateur l'introduction de nouvelles exceptions au principe de transparence, en soustrayant certaines activités de surveillance ou certaines catégories de documents officiels[18] sans qu'il ne soit réellement démontré en quoi les exceptions prévues dans la loi sont insuffisantes pour préserver le secret lorsque cela se justifie.

Enfin l'accès aux documents officiels contenant des données personnelles du demandeur est régi par les articles 8 et suivants de la loi fédérale du 19 juin 1992 sur la protection des données (LPD)[19]. Cette exception peut soulever en pratique des difficultés sur lesquelles je reviendrai ci-après[20]. L'article 4 LTrans réserve également les dispositions spéciales d'autres lois fédérales au sens formel qui peuvent empêcher l'accès, le soumettre à des règles plus strictes ou au contraire faciliter la consultation d'un document[21]. Sont visées en particulier des normes spéciales de secret.

15 Recommandation du PFPDT du 12 mai 2015, c. 31 ss ; PFPDT, FAQ 2.2.3.

16 Art. 3 al. 1 let. b LTrans.

17 Art. 67 LRens.

18 Le projet de loi concernant l'organisation de l'infrastructure ferroviaire (OBI) adopté par le Conseil fédéral le 16 novembre 2016 prévoit ainsi de soustraire à la LTrans les rapports d'audit et de contrôle de l'Office fédéral des transports, disponible en ligne sur : https://www.edoeb.admin.ch/aktuell/01432/index.html?lang=fr.

19 RS 235.1.

20 Voir II. E 2. e) ci-dessous.

21 FF 2003 1832.

C. Notion de document officiel

Une demande d'accès au sens de la LTrans doit viser des informations contenues dans un document officiel. Les autres documents échappent au champ d'application de la loi. L'article 5 LTrans définit ce qu'il faut comprendre par document officiel. Il s'agit de toute information qui a été enregistrée sur un quelconque support (papier, support numérique ou analogique, enregistrement audio, etc.), qui est détenue par l'autorité dont elle émane ou à laquelle elle a été communiquée et qui concerne l'accomplissement d'une tâche publique de la Confédération. Ces trois conditions s'appliquent de manière cumulative[22]. Si une de ces conditions n'est pas remplie, il ne peut y avoir d'accès au document souhaité sous l'angle du principe de la transparence[23]. La qualité du support n'est pas déterminante. Par contre, ce support doit avoir un contenu informatif, c'est-à-dire qu'il doit contenir des informations. Un disque dur ou une clef USB vierges ne constituent pas un document officiel. En outre, l'information doit exister[24]. Par contre un document virtuel peut, selon l'article 5 alinéa 2 LTrans, constituer un document officiel s'il peut être élaboré par un traitement informatisé simple sur la base d'informations existantes enregistrées. Selon le Tribunal administratif fédéral « *Gedacht hat [der Gesetzgeber] dabei in erster Linie an elektronische Datenbanken, in denen der begehrte Auszug als Dokument nicht existiert, die vorhandene Software jedoch darauf ausgerichtet ist, solche Auszüge zu generieren […]. Der Bundesrat hat hierzu in der Botschaft zum Bundesgesetz über die öffentliche Verwaltung vom 12. Februar 2003 lediglich festgehalten, der Begriff des einfachen elektronischen Vorgangs beziehe sich auf den Gebrauch durch einen durchschnittlichen Benutzer und könne deshalb durch die fortschreitende technische Entwicklung Änderungen erfahren […].Daraus ist zu folgern, dass der für die Generierung eines Dokumentes im Sinne von Art. 5 Abs. 2 BGÖ erforderliche Vorgang durchaus mehrere Arbeitsschritte umfassen kann, solange ein gewöhnlicher Benutzer ohne spezielle Computerkenntnisse das gewünschte Dokument hierdurch aus vorhandenen Informationen generieren kann.* »[25]. L'établissement d'une liste de noms de collaborateurs d'une autorité peut constituer un traitement informatisé simple sur la base d'informations enregistrées[26].

22 TAF A-1156/2011 du 22 décembre 2011, c. 8.3.2
23 BÜHLER, N 6 *ad* art. 5 LTrans.
24 BÜHLER, N 10 *ad* art. 5 LTrans.
25 TAF A-3363/2012 du 22 avril 2012, c. 3.5.1.
26 TAF A-6054/2013 du 18 mai 2015, c. 4.1.

1. Autres documents

Aux termes de l'article 5 alinéa 3 LTrans, ne rentrent pas dans la catégorie de documents officiels, les documents qui sont commercialisés par une autorité ou qui n'ont pas atteint leur stade définitif d'élaboration. Un document a atteint son stade définitif d'élaboration lorsque l'autorité dont il émane l'a signé ou lorsque son auteur l'a définitivement remis au destinataire[27]. La condition de l'état d'achèvement d'un document permet d'exclure de l'accès notamment des versions préliminaires d'un document. Seul compte et est susceptible d'être rendu accessible, un document achevé et définitif, par exemple la version finale d'une interview donnée par une conseillère fédérale[28] ; les versions antérieures contenant des corrections visibles ne constituent pas un document officiel.

2. Document à l'usage personnel

L'article 5 alinéa 3 lettre c LTrans exclut également de la notion de document officiel, les documents qui sont destinés à l'usage personnel. Cela vise toute information qui bien qu'établie à des fins professionnelles, est utilisée exclusivement par son auteur ou par un cercle restreint de personnes comme moyen auxiliaire (notes, copies de travail, etc.)[29]. Un document ne sera un auxiliaire que s'il est effectivement établi pour l'exécution d'une tâche et utilisé ainsi[30]. Comme le relève le PFPDT dans sa pratique, dans cette catégorie sont comprises toutes les informations qui servent les intérêts du service et ne sont utilisées et réservées qu'à l'auteur du document ou à un cercle très restreint de personnes. Sont ainsi visées des notes manuscrites, des propositions de corrections, des résumés, des réflexions, des notes de séance ou de travail qui servent d'instrument de travail à l'intérieur d'une équipe ou qui sont échangés entre collaborateurs, respectivement entre un collaborateur et son chef. En d'autres termes, il s'agit d'un instrument de travail, c'est-à-dire d'un document élaboré en cours de réalisation du travail[31].

Lorsqu'elles constituent en effet des informations utilisées exclusivement à des fins personnelles, certaines catégories de données personnelles, du moins celles qui ont un lien étroit avec des employés de l'administration, échappent au champ d'application de la LTrans. Ces données ne sont pas un document officiel selon l'article 5 alinéa 3 lettre c LTrans et 1 alinéa 3 OTrans [32]. Il s'agit notamment de notes personnelles ou « des lettres ou courriers électroniques qui sont adressés personnellement à un collaborateur de

---

27 Art. 1 al. 2 OTrans.
28 TAF A-1156/2011 du 22 décembre 2011, c.8.3.2.
29 Art. 1 al. 3 OTrans.
30 BÜHLER, N 29 *ad* art. 5 LTrans.
31 Recommandation du PFPDT du 23 décembre 2010, c. 3.1.
32 FLÜCKIGER, N 8 *ad* art. 9 LTrans.

l'administration et qui ne relèvent pas des affaires de service […] En revanche, les lettres personnelles à contenu officiel constituent des documents officiels puisqu'elles sont bel et bien destinées à l'usage officiel»[33]. Ne sont également pas considérés comme documents officiels, les documents contenant des données personnelles fournies à l'administration par des tiers et qui revêtent un caractère purement personnel ou privé et qui ne concernent pas l'accomplissement d'une tâche publique[34]. Ne sera ainsi pas considérée comme un document officiel une carte postale envoyée par un collaborateur à ses collègues depuis son lieu de vacances. De même si la liste des destinataires de cartes de vœux établies en exécution de tâches de représentation doit être considérée comme un document officiel, il n'en va pas de même de la liste de correspondants privés (amis) d'un magistrat, même si l'envoi de cartes de vœux est confié à son secrétariat[35].

D. Droit d'accès à un document officiel

Aux termes de l'article 6 alinéa 1 LTrans, « toute personne a le droit de consulter des documents officiels et d'obtenir des renseignements sur leur contenu de la part des autorités ». La consultation peut se faire sur place ou le demandeur peut requérir une copie[36]. La demande peut être adressée par courrier postal, par mail ou par oral. Le demandeur peut en principe demeurer anonyme[37]. La demande ne doit pas être motivée, mais contenir les indications suffisantes pour permettre d'identifier le document demandé.[38]. Cette disposition « constitue le cœur de la loi sur la transparence […] [elle] vient renverser [le] principe du secret de l'administration sous réserve d'exceptions pour ériger en principe celui de la transparence. »[39]. Il s'agit d'un changement de paradigme dans la pratique administrative qui ne reconnaissait aucun droit subjectif de la personne d'être informée des activités de l'administration[40]. Avec ce changement de paradigme, la LTrans établit une présomption d'accès aux documents officiels. Il y a un renversement du fardeau de la preuve. Il revient ainsi à l'administration de démontrer qu'un des motifs de restriction des articles 7 et 8 est rempli[41]. En cas de limitation ou de refus de l'accès, l'autorité doit motiver sa restriction. Elle ne peut se contenter de citer à la lettre les termes

33 FF 2003 1842.
34 FF 2003 1836.
35 R. J. SCHWEIZER, avis de droit non publié à l'adresse de la Chancellerie fédérale du 17 juin 2013.
36 Art. 6 al. 2 LTrans.
37 Toutefois, l'identité d'un demandeur peut être vérifiée à l'entrée d'un bâtiment de l'autorité, art. 4 al. 3 OTrans.
38 Art. 7 al. 1 et 2 OTrans.
39 FF 2003 1843.
40 MAHON/GONIN, N 1 ss *ad* art. 6 LTrans et auteurs cités.
41 MAHON/GONIN, N 11 *ad* art. 6 LTrans.

des exceptions énoncées dans LTrans ; elle doit motiver de façon à ce que le demandeur puisse comprendre les motifs d'une restriction[42]. Ce qui implique qu'elle examine chaque cas d'espèce et démontre en quoi l'accès peut porter atteinte à un intérêt ou un droit protégé. Toutefois suivant l'ampleur du document requis, il est admissible de catégoriser les motifs de restriction pour des faits similaires. Conformément au principe de proportionnalité, l'examen de l'existence ou de l'absence d'un intérêt public prépondérant ne peut en effet être effectué avec la même intensité que si la demande se limite à des inscriptions ou des informations spécifiques[43]. L'atteinte résultant de l'accès doit revêtir une certaine intensité et elle doit selon le cours ordinaire des choses se réaliser de manière hautement vraisemblable[44]. En cas de doute sur l'octroi ou non de l'accès, le principe de la transparence postule de donner l'accès[45]. Il revient à l'autorité de démontrer en quoi un document ne peut être rendu accessible[46].

1. Limitation de l'accès à un document officiel

Le principe de la transparence n'est pas absolu. Il l'emporte que dans la mesure où d'autres intérêts ou droits et libertés fondamentales ne s'opposent pas légitimement à l'octroi de l'accès. Il s'agit en particulier de concilier à la fois le principe de transparence et le respect du droit à la protection des données. Ainsi en présence d'une demande d'accès à un document officiel contenant des données personnelles ou portant sur des données personnelles, l'autorité requise doit, si possible, rendre les données personnelles anonymes avant que le document ne puisse être consulté[47]. Au préalable, l'autorité examinera tout d'abord s'il s'agit bien d'une demande sous l'angle de la LTrans ou s'il s'agit d'une demande de droit d'accès à ses propres données, auquel cas conformément à l'article 3 alinéa 2 LTrans, la demande sera traitée selon les articles 8 et suivant LPD. Plus problématique nous le verrons sont les demandes mixtes, c'est-à-dire celles portant sur un document officiel contenant à la fois des données personnelles du demandeur et des données de tiers. Une fois la question du sujet des données clarifiées et avant d'examiner la question de la possibilité de rendre anonyme les données, l'autorité se doit de vérifier au préalable si le document demandé entre dans le champ d'application de la loi et s'il s'agit bien d'un document officiel.

---

42 AMMANN/LANG, N 25.36.

43 TF 1C_14/2016 du 23 juin 2016, c. 3.3 et renvois.

44 Recommandation du PFPDT du 22 décembre 2016, c. 22 ; TF 1C_14/2016 du 23 juin 2016, c. 3.4 ; TAF A-3829/2015 du 26 novembre 2015, c. 3.2 et A-6291/2013 du 28 octobre 2014, c.7.

45 AMMANN/LANG, N 25.7 et 25.37, auteurs et jurisprudence cités.

46 TF 1C_14/2016 du 23 juin 2016, c. 3.4.

47 Art. 9 al. 1 LTrans.

S'il s'agit d'un document officiel soumis à la LTrans, l'autorité, par souci d'économie de procédure, examinera en premier lieu si aucune des exceptions prévues par la loi, à savoir, dispositions particulières de secret, intérêts publics essentiels ou intérêt manifestement dignes de protection de tiers, au sens des articles 4, 7, 8 LTrans, resp. 19 al. 4 LPD[48] ne sont remplies dans le cas d'espèce.

L'article 7 alinéas 1 et 2 LTrans en particulier énonce de manière exhaustive 9 cas d'intérêts publics ou privés qui peuvent justifier une exception au principe de transparence, sous forme de refus, de limitation ou d'ajournement de l'accès au document officiel demandé. Selon l'article 7 alinéa 1 LTrans, l'accès peut être limité, différé ou refusé lorsqu'on est en présence d'un :

- risque notable d'atteinte au processus de libre formation de l'opinion et de la volonté de l'autorité ;
- risque d'entrave à l'exécution de mesures concrètes prises par l'autorité ;
- risque de compromission de la sûreté intérieure ou extérieure de la Suisse ;
- risque de compromission des intérêts de la Suisse en matière de politique extérieure et ses relations internationales ;
- risque de compromission des relations entre la Confédération et les cantons ou les relations entre cantons ;
- risque de compromission des intérêts de la politique économique et monétaire de la Suisse :
- risque de révélation de secrets professionnels, d'affaires ou de fabrication ;
- divulgation des informations fournies librement par un tiers à une autorité qui en a garanti expressément le secret.

Ces deux dernières conditions sont aussi pertinentes du point de la protection des données.

L'article 7 alinéa 2 concerne le respect de la sphère privée de tiers. Il sera examiné que pour autant qu'aucun des autres motifs de restriction ne soit opposable. L'autorité se doit dans chaque cas d'examiner si un risque existe que l'un des intérêts mentionnés à l'article 7 soit atteint en cas d'octroi de l'accès. Le risque doit être sérieux et sa réalisation présenter un haut degré de vraisemblance. Il ne peut s'agir d'une simple supposition ou estimation[49]. Comme en matière de restrictions aux droits et libertés fondamentales, les clauses d'exception doivent être interprétées de manière restrictive afin de ne pas vider de

[48] La question de l'application de l'art. 19 al. 4 LPD n'est à considérer que si les données ne peuvent pas être anonymisées.

[49] COTTIER/SCHWEIZER/WIDMER, N 4 *ad* art. 7 LTrans.

son sens le principe de la transparence ; en cas de doute, il faut trancher en faveur de la transparence[50].

Si aucune des exceptions de l'article 7 alinéa 1 LTrans n'entre en ligne de compte et avant d'aborder l'article 7 alinéa 2 LTrans, l'autorité devrait encore avoir au préalable examiné si le document entre dans le cadre de l'article 8 LTrans, lequel stipule que le droit d'accès n'est pas reconnu pour les documents officiels afférents à la procédure de corapport ou pour les documents officiels de la procédure de consultation après la décision si le Conseil fédéral en a exceptionnellement ainsi décidé. Cette exception est applicable indépendamment de l'existence ou non de tout autre type d'exception. En revanche comme le relève le Tribunal fédéral dans l'arrêt *Reumann/Goumaz c. DFJP* au sujet des conventions de départ du secrétaire général du DFJP et de son suppléant[51], les documents qui accompagnent la proposition au Conseil fédéral ne sont pas en tant que tels soumis au secret instauré à l'article 8 alinéa 1 LTrans. Ainsi, le projet de proposition élaboré par un office fédéral à l'attention d'un département ne fait l'objet que de la restriction provisoire instaurée à l'article 8 alinéa 2 LTrans52 et peut être en soi rendu accessible une fois prise la décision politique ou administrative dont il constitue la base pour autant qu'aucune autre exception ne soit applicable. Pour éviter qu'en pratique toute information tombe sous cette exception, le document qui sert de base à une décision politique ou administrative doit être en étroite relation avec la décision à prendre et être pour celle-ci d'une importance matérielle significative[53]. Cela implique également que le document est un lien temporel étroit avec la décision à prendre. « *Il n'est donc pas admissible qu'une autorité retienne un document sous prétexte qu'il pourrait éventuellement constituer à l'avenir une base pour une décision fondamentale. Bien plutôt, l'autorité doit pouvoir attester qu'une décision sera prise dans un délai prévisible ou que le dossier en cause fait encore l'objet d'une élaboration en vue d'une décision à prendre.* »[54].

2. Accès à des données personnelles

Si elle parvient à la conclusion qu'aucun de ces motifs de restriction ou de refus de l'accès n'est rempli, avant d'envisager une restriction pour protéger la sphère privée de tiers conformément à l'article 7 alinéa 2 LTrans ou de considérer la possibilité d'anonymiser les données personnelles conformément à l'article 9 LTrans, l'autorité examinera la communication sous l'angle de l'article 19 alinéas 1 et 2 LPD, même si cela ne ressort pas expressément de la LTrans. Elle vérifiera tout d'abord si la personne concernée a consenti

---

50 *Ibidem*.

51 ATF 136 II 399 (404), c. 2.3.3.

52 MAHON/GONIN, N 19 *ad* art. 8 LTrans.

53 MAHON/GONIN, N 30 *ad* art. 8 LTrans ; TAF A-3631/2009 du 15 septembre 2009, c. 3.5.1 ; recommandation du PFPDT du 18 décembre 2007, c.3.

54 Recommandation précitée, c. 3.

à la communication de ses données ou les a rendues accessibles à tout un chacun et ne s'est pas opposée au traitement (article 19 alinéa 1 lettres b et c LPD). Elle examinera également si le destinataire a rendu vraisemblable que la personne concernée ne refuse son accord ou ne s'oppose à la communication que dans le but de l'empêcher de se prévaloir de prétentions juridiques ou de faire valoir d'autres intérêts légitimes. Elle vérifiera enfin si la demande ne porte pas uniquement sur le nom, le prénom et l'adresse de la personne concernée (article 19 alinéa 2 LPD). Dans cette dernière hypothèse, elle examinera encore s'il y a un motif de restriction au sens de l'article 19 alinéa 4 LPD, à savoir si un important intérêt public, un intérêt légitime manifeste de la personne concernée, une obligation légale de garder le secret ou une disposition particulière relevant de la protection des données l'exige. Relevons cependant qu'à l'exception de l'atteinte à la sphère privée de l'article 7 alinéa 2 LTrans, que la latitude pour appliquer l'article 19 alinéa 4 LPD devrait être très mince, voire inexistante si aucune restriction au sens des articles 4 et 7 alinéa 1 LTrans n'a pu être raisonnablement invoquée. Elle examinera également si aucune base légale au sens de l'article 17 alinéa 1 LPD en relation avec l'article 19 alinéa 1 n'autorise la communication des données demandées. Ce n'est qu'ensuite qu'il conviendra de considérer l'article 7 alinéa 2, respectivement les articles 9 LTrans et 19 alinéa 1bis LPD. Ainsi même si les conditions de l'article 19 alinéa 1 LPD ne sont pas remplies, l'accès à un document officiel contenant des données personnelles pourrait être accordé lorsque l'intérêt public l'emporte sur l'intérêt au maintien du secret[55].

Selon l'article 7 alinéa 2 LTrans, l'accès à des documents officiels peut être restreint, différé ou refusé s'il risque de porter atteinte à la sphère privée de tiers. C'est en règle générale le cas en présence de documents qui contiennent des données personnelles. La LTrans accorde ainsi une valeur importante au respect de la sphère privée, sans pour autant en faire un absolu ; si l'intérêt public l'emporte, il est possible de porter atteinte, de manière certes exceptionnelle, à la sphère privée des personnes concernées par les informations[56].

a) Notion de données personnelles

La LTrans ne définit pas les données personnelles mais renvoie à la LPD[57]. Il s'agit de toutes informations relatives à une personne physique ou morale identifiée ou identifiable. Elle couvre tout type de données personnelles, y compris les données sensibles[58], à savoir les données personnelles sur les opinions ou activités religieuses, philosophiques,

55 DFJP, Rapport explicatif, p. 24.
56 AMMANN/LANG, N 25.49.
57 Art. 3 let. a LPD.
58 Art. 3 let. c LPD.

politiques ou syndicales, la santé, la sphère intime ou l'appartenance à une race, des mesures d'aide sociale, ainsi que des poursuites ou sanctions pénales et administratives. Cela couvre également les profils de personnalité[59], c'est-à-dire un assemblage de données qui permet d'apprécier les caractéristiques essentielles de la personnalité d'une personne physique. Toute révélation d'un document contenant des données personnelles ne porte pas obligatoirement atteinte à la sphère privée d'un tiers. En particulier, il faut retenir comme document officiel contenant des données personnelles uniquement ceux qui contiennent des informations sur une ou plusieurs personnes, notamment des jugements ou des appréciations relatives à des personnes identifiées ou identifiables. Cela vise également des documents décrivant le comportement d'une personne et dont la communication pourrait lui être préjudiciable[60]. Par contre tout document mentionnant le nom d'une ou de plusieurs personnes n'est pas pour ce seul motif un document contenant des données personnelles. Rares sont en effet les pièces qui ne contiennent aucun nom de personne. Ne devrait ainsi pas être considéré comme un document contenant des données personnelles ou entraînant un risque d'atteinte à la sphère privée, un rapport ou une prise de position comportant le nom de son auteur, mais dont le contenu n'a aucun rapport avec lui[61]. Seuls peuvent être considérés comme documents officiels contenant des données personnelles, ceux dont les informations se réfèrent à une ou plusieurs personnes, nommément désignées ou aisément identifiables[62].

Nonobstant le risque d'atteinte à la sphère privée, l'accès peut néanmoins être accordé si l'intérêt public l'emporte sur l'intérêt au maintien du secret. « L'accès pourrait être accordé par exemple s'il s'agit de documents en rapport avec l'octroi d'avantages économiques substantiels, s'ils se rapportent à des personnes titulaires d'autorisations ou de concessions ou encore s'il s'agit de contrats que l'Etat a conclus avec des privés »[63].

b) Anonymisation des données

Pour résoudre le conflit qui peut résulter entre la nécessité d'assurer la protection des données et l'intérêt du demandeur à accéder à des documents officiels, l'article 9 LTrans contient une règle de coordination avec la LPD. En présence de données personnelles et avant d'accorder l'accès si l'intérêt public le justifie, il convient d'examiner, en application du principe de proportionnalité et conformément à l'article 9 alinéa 1 LTrans, la possibilité de rendre les données anonymes, notamment par le biais du caviardage ou le recours à des

59 Art. 3 let. d LPD.
60 Flückiger, N 15 *ad* art. 9 LTrans ; DFJP, Rapport explicatif, p. 25.
61 Flückiger, N 14 *ad* art. 9 LTrans, p.190 ; DFJP, Rapport explicatif p. 25.
62 DFJP, Rapport explicatif, p. 25.
63 FF 20031854.

pseudonymes[64], à des codes ou des numéros non parlants, c'est-à-dire de sorte que les personnes concernées ne soient plus, selon le cours ordinaire des choses, identifiées ou identifiables[65]. L'anonymisation peut aussi intervenir en éliminant les passages du document qui permettraient d'identifier des personnes[66]. La réidentification nécessiterait des moyens et des coûts disproportionnés. Dans ce cas, les données ne tombent plus dans le champ d'application de la LPD, car des données anonymes ne sont plus des données personnelles. Toutefois, une certaine prudence reste de rigueur, car les technologies actuelles et notamment l'exploitation des mégadonnées permettent plus aisément de réidentifier des personnes. En cas d'utilisation de pseudonymes ou de codes, les clés de décodage ou les tabelles de concordance, lorsqu'ils existent, doivent être en mains de l'autorité. Les clés de chiffrement doivent être suffisamment sûres compte tenu de l'état de la technique[67]. L'utilisation du NAVS13 ne constituerait par exemple pas un code permettant de garantir l'anonymat des personnes concernées ; si ce numéro figure dans le document demandé, il devrait être également remplacé ou caviardé. Le degré d'anonymisation requis va aussi dépendre, en application du principe de la proportionnalité, de l'ampleur du risque d'atteinte à la sphère privée ou à d'autres droits ou libertés fondamentales des personnes concernées au cas où leur réidentification serait effectuée une fois le document transmis. Plus le risque d'atteinte est grand, plus la technique d'anonymisation utilisée doit être robuste[68]. L'autorité se doit dès lors de procéder à une évaluation des risques liés à une réidentification. Dans la mesure où l'anonymisation est insuffisante, les personnes demeurent identifiables et les données contenues dans le document demeurent ainsi des données personnelles soumises à la LPD. Ce sera le cas de données chiffrées ou codées, dont la clé de chiffrement ou le code peut être facilement déchiffré ou décodé[69].

Pour assurer l'esprit de la LTrans, il est important que le demandeur puisse identifier les passages du document qui ont été rendus anonymes. « Aussi, l'anonymisation ou le caviardage de passages bien déterminés doivent-ils être pratiqués de telle manière que le demandeur puisse constater de visu que des passages déterminés du document ont été masqués. À cette fin, l'autorité peut enduire de noir les passages en question ou les signaler d'une autre façon (par exemple, en introduisant des crochets assortis de points de suspension ([…]). Le fait d'enduire le texte d'une couche de blanc ne permet pas toujours d'indiquer à coup sûr les parties du texte et les passages précis qui ont été caviardés »[70].

---

64 Voir aussi l'exemple de Flückiger, N 2 *ad* art. 9 LTrans.
65 TAF A-1200/2012 du 27 novembre 2012, c. 3.3.
66 Flückiger, N 30 *ad* art. 9 LTrans.
67 FLÜCKIGER, N 30 *ad* art. 9 LTrans.
68 FLÜCKIGER, N 31 *ad* art. 9 LTrans.
69 *Ibidem*.
70 PFPDT, FAQ 6.2.2.

aa) Limite au devoir d'anonymisation

Le devoir d'anonymisation n'est pas absolu et doit être examiné à la lumière des circonstances du cas d'espèce ; il doit également tenir compte du principe de proportionnalité (art. 5 alinéa 2 Cst). Selon l'article 9 alinéa 1 LTrans, le devoir de rendre anonymes les données doit donc intervenir dans la mesure du possible. Cela laisse une certaine marge d'appréciation à l'autorité, sans pour autant que l'administration bénéficie d'une totale liberté. Elle se doit d'éviter l'arbitraire et respecter l'égalité de traitement et la proportionnalité[71]. Elle tiendra compte non seulement de la faisabilité technique de l'anonymisation, mais aussi de l'intensité de l'atteinte à la sphère privée à préserver eu égard à l'intérêt public pouvant en l'espèce justifier la divulgation du document contenant des données personnelles ou encore de l'existence de dispositions légales spécifiques pouvant justifier la communication de données personnelles, à l'exemple de l'article 19 alinéa 1 lettre b, c et d ou alinéa 2 LPD. En outre dès lors que la sphère privée de la personne concernée ou d'autres droits et libertés fondamentales ne sont pas affectés, le devoir de rendre les données anonymes tombe. Enfin, exiger de rendre systématiquement anonymes les données contenues dans un document officiel irait à l'encontre du principe de transparence de l'administration et de l'objectif poursuivi par l'article 1 LTrans. Cet objectif ne doit pas être mis en péril par une interprétation excessive de l'obligation d'anonymisation[72].

Dans certains cas, l'anonymisation peut constituer une mesure disproportionnée du droit d'accès, en particulier lorsque la demande d'accès porte sur des données personnelles[73], par exemple la demande porte sur une personne nommément mentionnée dans la requête d'accès[74] :

- Un demandeur souhaitait l'accès à des données d'émissions de CO^2 des gros importateurs automobiles pour l'année 2014. Les données requises portaient sur des données personnelles rendant l'anonymisation impossible. Une anonymisation aurait eu pour conséquence de rendre matériellement impossible l'accès au document demandé[75].
- Dans un autre cas concernant la commission fédérale de vaccination, le TAF a considéré, à juste titre, suivant en cela la recommandation du PFPDT, qu'il était impossible de *« rendre anonyme les déclarations d'intérêts des membres de la CFV,*

71 AMMANN/LANG, N 25.61. Voir aussi les exemples cités au 25.62.

72 AMMANN/LANG, N 25.63 et auteurs cités.

73 Recommandation du PFPDT du 9 septembre 2016, c. 37 et jurisprudence citée.

74 FF 2003 1858.

75 Voir aussi TF 1C_137/2016 du 27 juin 2016, c. 4.1 ; TF 1C_74/2015 du 2 décembre 2015 c.3.4 ; TF 1C_50/2015 du 2 décembre 2015 c.5.2.2 et auteurs cités.

car celles-ci n'ont de sens que si un lien peut être fait entre l'identité du déclarant et les intérêts – ou les absences d'intérêts – déclarés. En telle occurrence, l'art. 19 LPD s'applique (art. 9 al. 2, 1ère phrase LTrans). »[76].

L'anonymisation n'est également pas envisageable si la requête porte sur une personne dont le nom est mentionné par le demandeur[77]. Il en ira de même, lorsque l'anonymisation implique, pour rendre les personnes non identifiables, de cacher des passages entiers d'un document de sorte qu'il devient incompréhensible pour le lecteur. Dans ce cas si l'intérêt public ne justifie pas de transmettre le document avec des données personnelles, l'autorité devrait envisager, pour préserver l'identité des personnes concernées, conformément au principe de proportionnalité, de rédiger un résumé du document demandé[78]. Cette manière de faire pourrait cependant se heurter à la définition de document officiel de l'article 5 alinéa 1 lettre a, puisqu'il s'agirait d'un document non encore existant. Du fait que la plupart des documents sont aujourd'hui élaborés avec des moyens informatiques et enregistrés sur des supports numériques, un tel résumé devrait relever de l'article 5 alinéa 2, sauf à considérer que son élaboration ne puisse pas intervenir de manière simple. Cette voie devrait être envisagée en tous les cas lorsque l'intérêt public à la transmission du document est suffisamment élevé, sans pour autant qu'il justifie la divulgation de données personnelles[79].

c) Vie privée contre intérêt public

Conformément à l'article 9 alinéa 2 LTrans, lorsque l'anonymisation n'est ainsi pas envisageable ou possible ou l'est de manière insuffisante, l'accès au document demandé doit être examiné à la lumière de l'article 7 alinéa 2 LTrans et des dispositions de la loi fédérale sur la protection des données, en particulier l'article 19, notamment 19 alinéa 1bis. Ce n'est qu'à ce stade que la question de la pesée des intérêts doit être examinée. Le rapport entre l'article 7 alinéa 2 LTrans et l'article 9 alinéa 1 LTrans, resp. 19 alinéa 1bis LPD peut être sujet à différentes interprétations. Tous deux reflètent les droits énoncés à l'article 13 Cst. Ce qui est déterminant, c'est que sur la base de ces deux dispositions une pesée entre l'intérêt public à l'accès et la protection de la vie privée, resp. du droit à l'autodétermination informationnelle des personnes dont les données sont contenues dans le document officiel requis, est indispensable[80]. L'article 19 alinéa 1bis LPD permet d'octroyer l'accès à des documents officiels contenant des données personnelles, y

---

76 TAF A-3192/2010 du 17 juin 2011, c. 6 ; recommandation du PFPDT du février 2010, c. 5.

77 TAF A-3609/2010 du 17 février 2011, c. 4.3.

78 FLÜCKIGER, N 32 *ad* art. 9 LTrans.

79 Dans le même sens, FLÜCKIGER, N 32 *ad* art. 9 LTrans.

80 TF 1C_137/2016 du 27 juin 2016, c. 4.3 ; voir aussi TAF A-8073/2015 du 13 juillet 2016, c. 6.1.2 et renvois.

compris des données sensibles ou des profils de la personnalité même si cela n'est pas expressément mentionné dans la LTrans[81]. En effet comme cela ressort de l'exemple mentionné dans le message du Conseil fédéral[82] – la publication de rapport d'enquête administrative – l'intention du législateur était bien de ne pas faire de distinction en fonction de la nature des données personnelles contenues dans un document officiel et de créer avec l'article 19 alinéa 1bis LPD la base légale nécessaire à la communication de données sensibles ou profils de la personnalité. De tels rapports contiennent régulièrement des données relatives à des sanctions administratives ou pénales, qui sont des données sensibles[83].

Tant l'article 7 alinéa 2 LTrans que l'article 19 alinéa 1bis LPD prévoient que la communication de données personnelles est possible en présence d'un intérêt public prépondérant. L'article 19 alinéa 1bis LPD contient une 2e condition selon laquelle les données concernées doivent être en rapport avec l'accomplissement de tâches publiques. Ces deux conditions s'appliquent de manière cumulative. Cette deuxième condition ne figure pas explicitement à l'article 7 alinéa 2 LTrans, car elle découle de la définition de document officiel de l'article 5 LTrans.

aa) Accomplissement d'une tâche publique

Selon l'article 19 alinéa 1bis lettre a LPD, les données doivent être en relation avec l'accomplissement d'une tâche publique. Cette exigence permet de tenir compte du principe de finalité de l'article 4 alinéa 3 LPD[84]. Cette condition est aussi à relier avec la définition du document officiel de l'article 5 alinéa 1 lettre c LTrans, à savoir un document qui concerne l'accomplissement d'une tâche publique. Toutefois, comme le relève SCHEFER[85], l'invocation du principe de finalité dans ce contexte est sujette à caution. Il me semble plutôt que l'article 19bis doit être compris comme une base légale permettant de déroger au principe de finalité en permettant d'accorder l'accès à certaines conditions pour permettre de respecter la finalité de la LTrans. Le fait que le document ait été élaboré dans l'accomplissement d'une tâche publique signifie certes que les données ont été collectées en vue d'une finalité déterminée et légitime, mais en aucun que leur divulgation respecte la finalité initiale et soit compatible avec celle-ci. La disposition signifie que seuls des documents contenant des données personnelles traitées dans le cadre de l'accomplissement d'une tâche publique peuvent le cas échéant être rendus accessibles lors d'une demande d'accès sous l'angle de la LTrans. Cela exclut des documents, qui tout en remplissant la

81 FLÜCKIGER, N 10 *ad* art. 9 LTrans et auteur cité.
82 FF 2003 1874.
83 BRUNNER, FS Schweizer, p. 50.
84 PFPDT FAQ 3.2.2 ; SCHEFER, pp. 89 s et auteurs cités.
85 *Ibidem*.

deuxième condition de l'article 19bis LPD (intérêt public prépondérant) n'auraient pas été élaborés ou obtenus dans le cadre de l'accomplissement d'une tâche publique.

bb) Intérêt public prépondérant

Quant à l'intérêt public prépondérant, l'ordonnance du 24 mai 2006 sur le principe de la transparence dans l'administration définit de manière non exhaustive ce qu'il faut entendre par là. Aux termes de l'art. 6 al. 2 let. a OTrans, un intérêt public à la transparence est jugé prépondérant, par exemple :

- lorsque le droit d'accès à un document répond à un besoin particulier d'information de la part du public suite notamment à des événements importants. Des événements de nature politique peuvent être considérés comme des événements importants au sens de cette disposition[86].
- Il peut également s'agir d'événements particuliers touchant l'administration ou qui se déroulent au sein de l'administration, par exemple des pratiques illicites lors d'adjudication ou des cas de corruption[87].
- L'intérêt public peut aussi être reconnu lorsque le droit d'accès sert à protéger des intérêts publics, notamment l'ordre, la sécurité ou la santé publique[88].
- Il peut aussi y avoir un intérêt public prépondérant lorsque la personne, dont la sphère privée pourrait être atteinte par le droit d'accès à un document officiel, est liée à une autorité soumise à la loi sur la transparence par un rapport de fait ou de droit qui lui procure des avantages importants[89]. Tel pourrait être le cas lorsqu'une personne prend part de manière privilégiée à un acte de l'administration (p. ex. lors d'une audition ou en qualité d'expert[90]), lorsqu'elle est partie à un contrat avec une autorité, lorsqu' elle a obtenu une concession ou encore lorsqu'elle a obtenu des avantages d'une certaine importance, notamment financiers (p. ex. des subventions ou autres aides financières). Il y a dès lors un risque que celle-ci puisse obtenir un avantage, notamment d'ordre financier au détriment d'autres personnes. Dans de tels cas, la personne doit tenir compte du fait que des informations concernant ce rapport privilégié peuvent être publiées.
- Il en va de même pour les rapports de surveillance ou d'une activité exercée sur la base d'une autorisation[91]. Il s'agit par là d'éviter des spéculations sur la question de savoir

86 TAF A-3609/2010 du 17 février 2011, c. 4.2 ; COTTIER/ SCHWEIZER/ WIDMER, N 85, *ad* art. 7 LTrans.
87 AMMANN/LANG, N 25.93 et auteurs cités.
88 Art. 6 al. 2 let. b OTrans.
89 Art. 6 al. 3 let. c OTrans.
90 TF 1C 137/2016 du 27 juin 2016.
91 Commentaire OTrans, p. 7 ; voir aussi FF 2003 1854 ; PFPDT, FAQ 3.1.3.

si des avantages financiers ont été accordés à certaines personnes ou sur celle de savoir si des cas de corruption ou de pression se sont produits[92].

Par rapport à une demande d'accès concernant des documents relatifs à l'identité et aux activités d'experts privés appelés à se prononcer sur des autorisations de médicaments, le Tribunal fédéral estime que des experts d'entreprise jouent un rôle significatif dans l'intérêt public, à savoir que la procédure d'autorisation de médicaments sert la protection de la santé publique. Il y a dès lors un intérêt public important à ce que leurs qualifications ou d'éventuels conflits d'intérêts soient connus[93].

d) Atteinte à la vie privée

Pour déterminer si l'accès doit être accordé, l'autorité se doit de procéder au cas par cas à une minutieuse pesée des intérêts en présence. Elle devra identifier les intérêts privés qui pourraient justifier de maintenir le secret en refusant, restreignant ou différant l'accès afin de ne pas porter atteinte à la sphère privée des personnes concernées. Comme relevé précédemment, toute communication de données personnelles n'entraine pas obligatoirement une atteinte à la sphère privée. Une telle atteinte sera donnée quand il résulte de la communication une violation effective et d'une certaine intensité de la personnalité ou des droits et libertés fondamentales de la personne concernée[94]. Selon la jurisprudence, la menace de violation d'un intérêt privé ou public en cas d'accès ne doit certes pas être réalisée avec certitude, mais ne doit pas non plus être simplement imaginable ou possible. L'atteinte doit être sérieuse, ce qui exclut un simple désagrément ou une conséquence insignifiante[95]. L'autorité tiendra en particulier compte de la nature des données personnelles contenues dans le document sollicité. Elle se montrera d'autant plus prudente en face de données sensibles, de profils de la personnalité ou de données issues d'un profilage, c'est-à-dire toute exploitation de données personnelles ou non, consistant à analyser ou prédire les caractéristiques personnelles essentielles d'une personne, notamment son rendement au travail, sa situation économique, sa santé, sa sphère intime ou ses déplacements[96]. Ces données doivent bénéficier d'une protection accrue et dans la pondération des intérêts en jeu, l'intérêt de la personne doit l'emporter sur l'intérêt public à l'accès[97]. Selon la jurisprudence et la doctrine, il convient d'accorder un poids plus élevé en faveur du maintien de la confidentialité de documents contenant

92 AMMANN/LANG, N 25.76 et jurisprudence citée.
93 TF 1C_137/2016 du 27 juin 2016, c. 4.6.
94 AMMANN/LANG, N 25.79 et auteurs cités.
95 TF 1C 137/2016, c. 2.2 ; voir aussi ATF 133 II 209, c. 2.3.3 ; TF 1C_14/2016 du 23 juin 2016 c. 3.4 et 1C_74/2015 du 2 décembre 2015 c. 4.1.3.
96 Art. 3 let. f ; Avant-projet de révision de la LPD.
97 TAF A-3609/2010 du 17 février 2011, c. 4.4.

des données sensibles de sorte que leur divulgation ne peut guère être envisagée[98]. Le TAF précise : « *Il sied aussi de prendre en compte les conséquences que l'accès aux documents officiels pourrait avoir sur la personne concernée. L'autorité compétente doit ainsi admettre le droit d'accéder aux données requises, lorsque celui-ci ne causera vraisemblablement aucune atteinte à la sphère privée de la personne en cause […]. Il en est de même lorsque la consultation des documents n'aura qu'une simple conséquence désagréable ou moindre sur cette personne[...] Lorsque l'atteinte à la sphère privée n'est qu'envisageable ou peu probable […], le droit d'accès doit aussi être accordé... En outre, les personnes occupant des positions élevées au sein de la hiérarchie administrative doivent davantage s'accommoder de la publication de leurs données personnelles que les employés exerçant des fonctions subalternes* »[99]. Dans le cas d'espèce, l'accès était demandé aux conventions de départ du secrétaire général du DFJP et de son suppléant. Le TAF a estimé à juste titre que les documents demandés ne comportaient pas de données sensibles et ne constituaient pas un profil de la personnalité. Si le fait de divulguer ces documents pouvait être ressenti comme désagréable pour les personnes concernées, il n'aurait pas de conséquence importante pour les concernés qui de surcroît du fait des hautes fonctions qu'ils occupaient devaient s'accommoder davantage d'une atteinte à leur sphère privée. En outre en octroyant l'accès, l'autorité permettait au requérant et au public en général de vérifier le respect ou le non-respect des dispositions de la législation fédérale sur le personnel de la Confédération[100]. En ce sens, il y avait donc un intérêt public à l'accès qui l'emporte sur l'intérêt la protection de la sphère privée.

L'intérêt public à la communication sera également en règle générale donné et il ne sera pas nécessaire d'anonymiser les données personnelles lorsqu'elles concernent des personnes ayant une fonction officielle et accomplissant une tâche publique (par exemple des membres de commissions ou des employés de la Confédération)[101]. Dans l'exercice de leur fonction, ils ne peuvent ainsi se prévaloir d'une protection étendue de leur sphère privée. Cela pourrait être le cas lorsqu'il s'agit de révéler qui agit dans une fonction publique et soutient quelle opinion[102].

En revanche, il y a lieu de renoncer à toute communication « si elle a ou peut avoir selon une grande probabilité des conséquences négatives concrètes pour l'employé de l'autorité […] Il va de soi par exemple que les dossiers personnels des employés de la Confédération

98 TAF A-6054/2013 du 18 mai 2015, c 4.4.2 ; voir aussi TAF A-5111/2013 du 6 août 2014, c. 7.1 et renvois.

99 TAF A-3609/2010 du 17 février 2011, c. 4.4 et auteurs cités.

100 TAF A-3609/2010 du 17 février 2011, c. 5.4 et 5.5.

101 AMMANN/LANG, N 26.62 et auteurs cités.

102 PFPDT, FAQ 5.2.3 ; Recommandation du PFPDT du 3 septembre 2013, c. 24.

ne sont pas en règle générale accessibles »[103]. De même il n'y a pas lieu de communiquer des appréciations relatives à des chercheurs dans le cadre de l'examen de projet de recherche portant notamment sur leur parcours académique et leurs compétences spécifiques[104].

aa) Intensité de l'atteinte

L'appréciation de l'intensité de l'atteinte à la sphère privée peut se faire sur la base de différents critères. Outre la nature des données déjà évoquée, le fait que la collecte par l'autorité repose sur une obligation légale – par exemple lors de l'exercice d'une tâche de surveillance sur un privé – peut justifier de faire primer la protection de la sphère privée[105]. Il en ira de même si la personne a communiqué de manière volontaire des données la concernant à une autorité et obtenu de celle-ci la garantie explicite que la confidentialité serait respectée conformément à l'article 7 alinéa 1 lettre h LTrans[106]. Cette assurance justifie en règle générale de refuser l'accès, sauf à pouvoir rendre les données anonymes.

La fonction ou la position de la personne concernée – nous l'avons évoqué – joue également un rôle. Ainsi on tiendra compte de la position hiérarchique des personnes concernées. Un directeur d'office, un secrétaire général d'un département ou un homme politique ne jouira pas de la même protection qu'un subalterne, en particulier un collaborateur sans responsabilité de gestion ou d'une personne qui n'est pas dans une situation privilégiée par rapport à l'autorité. Le fait qu'une personne ne soit pas connue du public ou qu'elle le soit joue également un rôle[107]. Toutefois, le fait qu'une personne soit connue du public ne justifie pas à lui seul l'octroi de l'accès. Celle-ci a également droit au respect de sa vie privée. La balance réside dans la contribution que la connaissance de l'information peut apporter à l'objectif de la transparence.

e) Accès à ses propres données et à celles de tiers

La LTrans ne s'applique qu'aux documents contenant des données personnelles de tiers. Si la demande d'accès porte sur un document contenant uniquement des données personnelles du demandeur, la requête ne tombe pas sous la LTrans, mais relève des articles 8 et 9 LPD (droit d'accès) comme cela est précisé à l'article 3 alinéa 2 LTrans. Ce sera le cas par exemple lorsque le demandeur requiert l'accès à la correspondance qu'il a entretenue avec l'autorité requise[108]. Cela implique que l'autorité puisse établir que les

---

103 PFPDT, FAQ 5.2.3.
104 TF 1C_74/2015 du 2 décembre 2015.
105 COTTIER/SCHWEIZER/WIDMER, N 82 *ad* art. 7 LTrans.
106 AMMANN/LANG, N 25.82 ; COTTIER/SCHWEIZER/WIDMER, N 46 ss *ad* art 7 LTrans.
107 Voir aussi ATF 137 I 16, c. 2.5 avec renvoi.
108 Recommandation PFPDT du 27 mai 2015, c. 24.

données personnelles contenues dans le document sont bien celles du demandeur. Cela est possible si celui-ci est clairement identifié. Mais celui-ci n'a pas l'obligation de le faire, contrairement à une demande au sens de l'article 8 LPD. L'autorité doit également pouvoir établir si l'accès concerne uniquement les données personnelles du demandeur ou si la demande porte sur l'ensemble des informations du ou des documents demandés. Plus problématique est le cas de demande qui concerne à la fois ses propres données et celles de tiers. A priori la demande pourrait être traitée autant sous l'angle de la LTrans, avec le risque pour la personne concernée en cas de réponse positive que toute autre demande ultérieure portant sur le même document soit également transmis par la suite à des tiers. Si par contre, on applique la LPD, il est possible, dans la mesure où aucun motif de restriction de l'article 9 LPD ne s'applique, de donner l'accès à la personne concernée à ses propres données, tout en restreignant ou refusant l'accès aux données de tiers lorsque leurs intérêts prépondérants sont menacés (article 9 alinéa b LPD). Dans ce cas même si la LPD ne l'exige pas expressément, la protection des intérêts prépondérants peut être également atteinte en anonymisant les données des tiers. Pour la personne concernée, l'application de la LPD peut ainsi s'avérer plus avantageuse. L'application de la LPD par contre pourrait s'avérer défavorable à la personne concernée si le document requis contient d'autres informations qui ne la concernent pas et qui tombent sous le coup d'une des exceptions de la LTrans. À mon sens, le choix entre l'une ou l'autre loi ne devrait pas être laissée uniquement à la personne concernée. Si la demande porte uniquement ou essentiellement sur un document contenant des données personnelles du requérant, l'administration appliquera la LPD, ce qui implique avant d'examiner la demande de droit d'accès d'avoir vérifié l'identité de la personne concernée[109]. Certes la LTrans n'exige pas d'identifier le demandeur qui peut déposer sa demande sans avoir à s'identifier. Il peut adresser sa demande par un simple mail, ce qui peut compliquer la tâche de l'administration. Si l'autorité ne s'assure pas que la demande porte bien sûr les données du demandeur, elle risque alors de divulguer des informations sur des tiers et de porter atteinte à leur sphère privée de manière illicite. En présence d'une demande portant sur ses propres données et sans s'assurer de l'identité de la personne, le demandeur pourrait obtenir de manière relativement aisée des données personnelles d'autres personnes[110]. Ainsi, je me demande si face à d'une demande d'accès à des documents officiels contenant des données personnelles, l'autorité ne doit pas en cas de doute sur le lien entre les données personnelles requises et la personne du demandeur pouvoir exiger de ce dernier qu'il précise sa demande et s'identifie.

Par contre si le demandeur s'intéresse essentiellement aux données des tiers ou à d'autres informations, la demande devrait être examinée sous l'angle de la LTrans, ne serait-ce que

[109] AMMANN/LANG, N 25.54 et 25.55.
[110] AMMANN/LANG, N 25.56.

du fait que l'identité du demandeur n'est pas déterminante pour examiner la demande au sens de la LTrans[111]. Dans ce cas, j'estime que si les données des tiers peuvent être anonymisées pour protéger leur sphère privée, il n'est pas nécessaire de le faire pour celles concernant le demandeur, car sa sphère privée n'est pas touchée. Mais cela implique d'être sûr de l'identité du demandeur. La question de l'anonymisation pourrait néanmoins se reposer en cas de demande ultérieure d'un tiers.

E. Jurisprudence concernant l'accès aux données des employés de la Confédération

La question de l'accès aux données personnelles lors d'une demande d'accès à un document officiel se pose régulièrement en relation avec des données concernant des employés de la Confédération, parfois d'entreprises privées, d'autres administrations ou organisations ou de personnalités publiques. Elle a fait l'objet de nombreuses recommandations du PFPDT et d'arrêts du TAF et du TF dont certains ont déjà été mentionnés auparavant. Je me limite ci-dessous à quelques exemples marquants.

1. Communication d'une liste de collaborateurs traitant des dossiers de la Comco

Dans un arrêt concernant l'accès à une liste nominative des collaborateurs/trices de la Comco ayant traité certains dossiers de fusion d'entreprises[112], le TAF souligne que dans la pesée d'intérêt, la fonction, respectivement la position d'une personne publique ou d'un employé d'État ayant un poste de gestion doit être appréciée différemment de celle d'un employé subordonné ou d'une personne privée. Les employés d'État qui remplissent des tâches publiques ou qui participent à leur exécution ne peuvent en principe pas bénéficier du même niveau de protection de leur droit à l'autodétermination informationnelle que des personnes privées. Des employés, même dans une position subordonnée, doivent ainsi s'attendre à ce que soit communiqué le nom de la personne qui a rédigé un document particulier ou qui a été en charge d'une affaire déterminée. Ces informations ne peuvent pas être anonymisées. Toutefois dans sa pesée d'intérêt, le TAF restreint le cercle des employés dont le nom peut être divulgué aux personnes qui ont pris une part déterminante au traitement des affaires en question, notamment comme conseiller ou comme instructeur. L'intérêt public à la transparence justifie en l'espèce de savoir qui a participé de manière déterminante à l'instruction des cas de fusion examinés par la Comco et a préparé les décisions de celle-ci. Le demandeur est en droit de se faire une opinion sur l'activité de la commission et de son secrétariat et, de cette manière, à pouvoir également vérifier son

111 FLÜCKIGER, N 18 *ad* art. 9 LTrans.
112 TAF A-6054/2013 du 18 mai 2015, c. 4.2.2 et renvois, c. 4.3.

indépendance. La communication du nom des collaborateurs ne peut en l'espèce avoir de désavantages concrets pour les intéressés. Elle peut tout au plus entrainer un minime désagrément qui n'est pas constitutif d'une atteinte à la vie privée. L'intérêt public ne justifie par contre pas de divulguer le nom des personnes qui n'ont joué qu'un rôle secondaire et qui n'ont pas eu une influence déterminante dans la prise de décision. Ces dernières doivent bénéficier d'une protection similaire à celle d'une personne privée.

2. Accès à l'agenda Outlook d'un haut fonctionnaire

Statuant sur un recours d'un journaliste souhaitant avoir accès à l'agenda électronique du directeur général de l'armement pour la période du 1er janvier 2013 au 26 mai 2014, le Tribunal fédéral[113] admet le caractère de document officiel d'un agenda. Ce document doit être considéré comme ayant atteint son stade définitif d'élaboration puisque la demande du journaliste portait sur une période déterminée révolue, ce d'autant plus que l'agenda ne donnait des informations que sur les rendez-vous et les séances, sans indiquer si ceux-ci se sont déroulés dans la manière prévue et planifiée. Le fait que le public puisse prendre connaissance d'indications de l'agenda qui ne correspondent pas toujours nécessairement avec le déroulement des événements n'entraine pas un danger significatif de malentendu. Les informations contenues dans l'agenda électronique Outlook décrivent l'activité de l'ancien chef de l'armement. Celui-ci a utilisé son agenda dans le cadre de l'exercice de ses fonctions et dès lors dans l'exercice d'une tâche publique. Même si l'agenda contient également des rendez-vous privés, les informations qui y sont enregistrées servent essentiellement les activités officielles et la direction de l'office. En outre, le fait que l'agenda n'est pas un document devant être archivé n'enlève rien à la qualification de document officiel entrant dans le champ d'application de la LTrans[114]. En outre l'agenda ne peut être en l'espèce qualifié de document destiné à l'usage personnel ; il ne s'agit pas d'un simple instrument personnel de gestion des rendez-vous, mais il constitue un instrument interactif central de la direction de l'office, même s'il est accessible à un cercle restreint de personnes. Il permet la planification des échéances, l'organisation et la communication au sein de l'office et au-delà. Le document requis contenait des données personnelles concernant notamment les personnes avec lesquelles ils projetaient de se rencontrer. L'autorité se doit dès lors d'accorder l'accès sous réserve qu'elle puisse justifier et motiver un intérêt public ou privé prépondérant, notamment le droit à la vie privée des personnes concernées pour refuser ou restreindre l'accès, par exemple en caviardant certaines informations. En particulier, il est en principe justifié de caviarder les rendez-vous et les manifestations de nature privée. En outre vu l'ampleur du document requis, il est admissible de catégoriser les motifs de restriction pour des faits similaires. Conformément au principe de proportionnalité, l'examen de l'existence ou de l'absence

113 TF 1C_14/2016 du 23 juin 2016.
114 TF 1C_14/2016 du 23 juin 2016, c. 2.2 et renvois.

d'un intérêt public prépondérant ne peut en effet être effectué avec la même intensité que si la demande se limitait à des inscriptions spécifiques de l'agenda. Dans l'appréciation des cas d'espèce, le Tribunal fédéral rappelle que les critères déterminant à prendre en considération sont la fonction ou la position de la personne concernée, la nature des données, l'existence d'un intérêt particulier à l'information du public, la protection d'intérêt spécifique, la nature des rapports entre l'administration et les tiers concernés, ainsi que l'importance de la thématique en question[115].

3. Demande d'accès à la liste des activités accessoires des employés fédéraux

Un journalise souhaitait l'accès à la liste des activités accessoires, annoncées et autorisées, des employés fédéraux qui sont enregistrés dans le système d'information du personnel BV-PLUS afin de vérifier si les règles concernant les activités accessoires sont correctement appliquées. Dans un arrêt du 23 septembre 2015, le TAF lui a donné partiellement raison[116]. La demande ne concernait pas un document officiel existant au sens de l'article 5 alinéa 1 LTrans. Les informations étaient néanmoins enregistrées dans un système d'information et permettaient d'établir un document par un traitement informatisé simple conformément à l'article 5 alinéa 2 LTrans. Un traitement informatisé simple consiste en un traitement que le logiciel permet et qu'un utilisateur moyen du système, sans connaissance informatique particulière, peut effectuer[117]. L'investissement nécessaire pour établir le document se limite au document à produire et non à l'ensemble de la procédure d'examen de la demande d'accès, notamment l'investissement pour la consultation éventuelle des personnes concernées au sens de l'article 11 LTrans. Dans la mesure où cet investissement est réduit, l'établissement du document virtuel au sens de l'article 5 alinéa 2 LTrans est possible.

Les données requises concernent des activités accessoires et ne constituent pas des données sensibles au sens de l'article 3 lettre c LPD, même si elles sont qualifiées de sensibles à l'article 27c alinéa 1 lettre h de la loi fédérale du 24 mars 2000 sur le personnel de la Confédération (LPers)[118]. Même si les employés d'État ne bénéficient en règle générale pas du même niveau de protection de leur droit à l'autodétermination informationnelle qu'une personne privée, lorsqu'ils agissent dans le cadre de leur fonction, les cadres assumant une fonction de gestion doivent néanmoins s'attendre à une protection moins élevée qui peut, le cas échéant, entrainer la communication de données sensibles. Ceci par contre ne doit normalement pas être le cas pour les employés des échelons inférieurs. Concernant l'exercice des activités accessoires, l'article 23 LPers prévoit que celles-ci

115 TF 1C_14/2016 du 23 juin 2016, c. 3.3 et renvois.
116 TAF A-6738/2014 du 23 septembre 2015.
117 TAF A-6738/2014 du 23 septembre 2015, c. 4.3.3.
118 RS 172.220.01.

peuvent être soumises à autorisation lorsque ces activités risquent de compromettre l'exécution de leurs tâches. Il s'agit de garantir l'utilisation optimale des ressources de la Confédération et de son personnel, d'assurer l'indépendance et la crédibilité de l'administration et éviter des conflits d'intérêts entre la Confédération, son personnel et des tiers. Il y a donc un intérêt public important à pouvoir vérifier la bonne application des dispositions sur les activités accessoires, ce qui peut justifier la communication des informations requises[119]. Le Tribunal estime néanmoins qu'il faut prévoir un traitement différent selon qu'il s'agit de cadre supérieur ou d'autres employés de l'État. Ainsi face aux cadres assumant des fonctions de gestion et qui disposent d'une compétence décisionnelle plus élevée, il s'avère particulièrement pertinent de révéler le nom et l'activité accessoire autorisée afin de permettre le contrôle effectif de la pratique suivie en matière d'autorisation de ces activités accessoires. On renoncera à communiquer le nom uniquement si la personne concernée subit un préjudice majeur ou le risque de survenance d'un tel dommage s'avère élevé. Dans le cas d'espèce, ce risque parait inexistant ou minime. Toutefois, avant de communiquer les informations, la consultation des personnes concernées doit être garantie conformément à l'article 11 LTrans. Pour les autres catégories d'employés, le Tribunal estime que l'intérêt public ne l'emporte pas sur leur droit à la protection des données, car ceux-ci ont moins d'influence dans le processus décisionnel et dès lors d'éventuels conflits d'intérêts portent moins à conséquence. Toutefois, s'il se justifie de ne pas communiquer le nom des employés, cela ne signifie pas pour autant qu'aucune information ne soit communiquée au demandeur, ce qui en l'espèce serait disproportionné et ne permettrait pas de vérifier la bonne application des dispositions légales. Conformément à l'article 9 alinéa 1 LTrans, il est possible de transmettre des données issues du système BV-Plus de manière anonyme se limitant à indiquer la fonction, le taux d'occupation et l'activité accessoire autorisée. Le nom de l'employeur auprès duquel l'activité accessoire est exercée doit également être rendu anonyme[120].

4. Demande d'accès aux résultats d'une enquête administrative

Dans son arrêt du 13 juillet 2016 concernant la communication d'un rapport sur une enquête administrative en relation avec des reproches adressés à un haut fonctionnaire[121], le TAF parvient à la conclusion qu'une partie des données de la personne concernée figurant dans le rapport d'enquête doivent être rendues anonymes avant qu'il ne soit transmis au requérant afin de minimiser les conséquences négatives pour cette dernière et tenir compte de la protection de sa personnalité. Il se justifie en particulier de ne pas mentionner le nom et la fonction ou autre dénomination, sans pour autant devoir garantir un anonymat complet dans le cas d'espèce. Une anonymisation complète du rapport

[119] TAF A-6738/2014 du 23 septembre 2015, c. 5.2.2 et renvois.
[120] TAF A-6738/2014 du 23 septembre 2015, c. 5.2.3 et renvois.
[121] TAF A-8073/2015 du 13 juillet 2016.

équivaudrait à un refus – au moins partiel – de la demande d'accès et amoindrirait considérablement la pertinence de l'information contenue dans le rapport. Le Tribunal réaffirme qu'en présence de données sensibles, mais également de profils de la personnalité, la balance dans le cadre de la pesée d'intérêt doit en règle générale pencher en faveur du droit à la protection des données et à la vie privée[122]. Confirmant sa jurisprudence constante, il rappelle néanmoins qu'il faut aussi prendre en considération la fonction et la position de la personne concernée. En outre, le fait que les reproches formulés à l'encontre du haut fonctionnaire aient été rendus publics dans la presse et ont amené l'autorité à mandater une enquête administrative est de nature à justifier l'intérêt public à donner l'accès aux résultats de l'enquête administrative. Le besoin de clarifier les reproches formulés à l'encontre de la personne concernée et le soupçon de dysfonctionnement de l'organisation interne confère un poids particulier à l'intérêt à la transparence. Le principe de transparence vise aussi au contrôle de l'administration et en particulier la conduite d'une enquête en renforce la nécessité. L'intérêt public concerne non seulement l'objet de l'enquête, mais également l'enquête elle-même en tant qu'activité administrative. Le public doit, sur la base du rapport d'enquête, pouvoir se faire une opinion sur sa conduite, les résultats et les conclusions en découlent. Les données personnelles concernent l'activité professionnelle du concerné au moment des faits. Elles ne sont pas de nature sensible et les reproches reproduits dans le rapport ne constituent, aux yeux du tribunal, également pas un profil de la personnalité. La nature des informations malgré un contenu partiellement accablant ne justifie pas un intérêt prépondérant au maintien du secret.

La personne concernée a occupé une position en vue dans l'administration qui peut justifier la communication des données et dès lors une atteinte à sa vie privée. Le fait qu'elle ait quitté ses fonctions et ne soit plus au centre de l'attention publique est de nature à relativiser sa position antérieure dans la pesée d'intérêt. Un droit à l'oubli d'une personnalité publique ne peut cependant être également reconnu que de manière restrictive et apprécié de cas en cas[123].

F. Droit d'être entendu

Lorsque suite à la pesée des intérêts en présence, en l'absence d'un motif de refuser l'accès ou en cas d'impossibilité de rendre les données anonymes, l'autorité parvient à la conclusion que l'intérêt public paraît de premier abord prépondérant et envisage donc de donner suite à une demande d'accès contenant des données personnelles de tiers, elle

[122] TAF A-8073/2015 du 13 juillet 2016, c. 6.1.3 et renvois.
[123] TAF A-8073/2015 du 13 juillet 2016, c. 6.2.3.2 et renvoi ; voir aussi WALTER, pp. 5 ss.

consulte la personne concernée et l'invite à se prononcer dans un délai de 10 jours conformément à l'article 11 alinéa 1 LTrans. Bien que la LTrans ne prévoit pas expressément d'exception à cette obligation de consulter, elle n'est pas absolue et l'autorité peut dans certains cas y renoncer[124]. Ce renoncement doit cependant être exceptionnel pour ne pas aller à l'encontre du respect des droits des personnes concernées et dès lors reposer sur un motif justificatif[125]. Dans son arrêt du 27 juin 2016 concernant l'accès à des documents concernant l'identité et les activités d'experts privés appelés à se prononcer sur les autorisations de médicaments[126], le Tribunal fédéral estime que le fait que la société recourante ait déjà fait valoir tous les intérêts privés pertinents s'opposant à l'accès, ne constituait pas un motif justificatif suffisant, car il ne reflétait pas l'ensemble des arguments que les experts concernés pouvaient faire valoir afin de protéger leur sphère privée. L'autorité n'était ainsi pas en mesure d'évaluer si la révélation des noms de certains experts pouvait nuire à leur carrière ou à leur réputation professionnelle. L'autorité renoncera à cette audition si la personne concernée a donné son consentement à la divulgation ou a rendu ses données accessibles à tout un chacun sans s'opposer à leur traitement ultérieur. Elle pourra renoncer également à une telle audition si cela est impossible (par exemple adresse inconnue) ou disproportionné (par exemple la demande concerne un trop grand nombre de personnes[127]) ou encore l'intérêt à l'information est qualifié et s'avère d'une actualité brisante ne justifiant pas de différer l'accès[128]. Il est également possible de renoncer à la consultation lorsque les données pertinentes ont déjà été précédemment publiées, comme par exemple dans le cadre d'une procédure d'adjudication[129]. La personne consultée peut prendre position, mais ne dispose pas d'un droit de veto. Sans être déterminant, son avis sera néanmoins un élément à prendre en considération dans la décision d'accorder ou de refuser l'accès. L'autorité informera la personne entendue de sa prise de position sur la demande d'accès[130]. Au cas où l'autorité compte donner une suite positive à la demande d'accès du demandeur, la personne concernée peut introduire une demande en médiation auprès du Préposé fédéral à la protection des données et à la transparence. La demande d'accès sera suspendue jusqu'à droit connu[131]. Mentionnons ici également que conformément à l'article 13 LTrans, le demandeur qui se voit refuser, restreindre ou différer l'accès à un document officiel doit également requérir la médiation du Préposé fédéral avant de pouvoir obtenir une décision

124 TF 1C/ 137/2016 du 27 juin 2016, c. 4.6.6 et auteurs cités.
125 TF 1C_50/2015 du 2 décembre 2015, c. 6.2.
126 TF 1C_137/2016 du 27 juin 2016, c. 4.6.8.
127 TF 1C_50/2015 du 2 décembre 2015, c. 6.2.
128 AMMAN/LANG, N 25.101 et auteurs cités.
129 TF 1C_50/2015 du 2 décembre 2015, c. 6.2.
130 Art. 11 al. 2 LTrans.
131 Art. 13 al. 1 let. c LTrans.

sujette à recours. Celui-ci examine le cas et si la médiation n'aboutit pas émet une recommandation à l'autorité[132]. Suite à la recommandation du Préposé, le demandeur et la personne concernée peuvent demander à l'autorité une décision sur l'accès[133]. Cette décision peut être attaquée devant le Tribunal administratif fédéral. L'autorité rend d'elle-même la décision si, en dérogation à la recommandation, elle entend limiter, différer ou refuser l'accès ou entend accorder le droit d'accès à un document contenant des données personnelles[134].

III. Conclusion

Le mécanisme de la loi sur la transparence n'affaiblit pas le droit à la vie privée et à la protection des données garanti par l'article 13 de la Constitution. En rapprochant le droit à la protection des données et le principe de la transparence, le législateur a voulu assurer un équilibre entre deux droits de valeur égale. Il ne devrait pas y avoir d'opposition entre deux impératifs démocratiques ; ces deux droits se doivent d'être complémentaires. Les autorités sont ainsi appelées à apprécier de cas en cas si l'intérêt à la transparence l'emporte sur le respect de la vie privée ou si le maintien de la confidentialité s'oppose à la divulgation des informations. Ces deux droits ne sont pas absolus et il est nécessaire de vérifier par une pondération d'intérêts si les avantages offerts par l'un priment les inconvénients et les risques liés à l'autre. Cela permet au travers de la pesée des intérêts en présence de donner l'accès à des documents officiels lorsque l'intérêt public prépondérant justifie une atteinte légitime au droit à la vie privée et à la protection des données. Dans nos sociétés, le fonctionnement de la démocratie implique parfois que certaines données personnelles traitées par des organes publics soient accessibles à tous et permettent de vérifier le bon fonctionnement des institutions.

Si en pratique la concurrence entre le droit à la transparence et le droit à la protection des données et à la sphère privée a pu être et peut être résolue par une saine pesée des intérêts en présence et trouver des réponses dans les nombreuses recommandations du Préposé fédéral et dans la jurisprudence du TAF et du TF, il me paraît néanmoins nécessaire après 10 ans d'application, de corriger les erreurs de jeunesse dans la conception de la loi et son articulation avec la loi fédérale sur la protection des données. En effet, le système est relativement complexe et l'application de deux lois, voire la relation entre l'article 7 alinéa 2 LTrans et l'article 9 alinéa 2 LTrans, resp. l'article 19bis LPD n'est pas toujours évidente. Personnellement, je serais favorable aujourd'hui à l'élaboration d'une seule loi

132 Art. 14 LTrans.
133 Art. 15 al. 1 LTrans.
134 Art. 15 al. 2 LTrans.

régissant l'accès aux documents officiels et la protection des données personnelles. À défaut, il serait judicieux de régler l'accès à des documents officiels contenant des données personnelles de tiers uniquement dans la LTrans, sans pour autant vouloir affaiblir le droit à la protection des données et à la sphère privée des personnes concernées.

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.

AMMANN RETO/LANG RENATE, Öffentlichkeitsgesetz und Datenschutz, *in* : Nicolas Passadelis/David Rosenthal/Hanspeter Thür (éds.), Datenschutzrecht – Handbücher für die Anwaltspraxis, Bâle 2015.

BRUNNER, STEPHAN C., Commentaire de l'art. 1 LTrans, *in* : Stephan C. Brunner/Luzius Mader (éds.), Öffentlichkeitsgesetz – Handkommentar, Berne 2008, pp. 27 ss.

BRUNNER, STEPHAN C., Commentaire de l'art. 26 PA, *in* : Christoph Auer/Marcus Müller/Benjamin Schindler (éds.), Kommentar zum Bundesgesetz über das Verwaltungsverfahren (VwVG), Berne 2008.

BRUNNER, STEPHAN C., Interessenabwägung im Vordergrund, Hinweise im Hinblick auf die praktische Anwendung des Öffentlichkeitsgesetzes auf Bundesebene, *in* : Digma 4/2004, pp. 160-164.

BRUNNER STEPHAN C., Öffentlichkeit der Verwaltung und informationelle Selbstbestimmung : von Kollisionen und Verkehrsregeln, *in* : Selbstbestimmung und Recht, FS für Raine J. Schweizer, Zurich 2003, pp. 50 ss (cité : BRUNNER, FS Schweizer).

BRUNNER STEPHAN C./FLÜCKIGER ALEXANDRE, Nochmals : Der Zugang zu amtlichen Dokumenten, die Personendaten enthalten, *in* : Jusletter 4 octobre 2010.

BÜHLER ROBERT, Commentaire de l'art. 5 LTrans, *in* : Urs Maurer-Lambrou/Gabor-Paul Blechta (éds.), Datenschutzgesetz/Öffentlichkeitsgesetz – Basler Kommentar, 3e édition, Bâle 2014.

CONSEIL FÉDÉRAL, Message relatif à la loi fédérale sur la transparence de l'administration du 12 février 2003 (LTrans), FF 2003 1807 (cité : Message LTrans).

COTTIER BERTIL/SCHWEIZER RAINER J./WIDMER NINA, Commentaire de l'art. 7 LTrans, *in* : Stephan C. Brunner/Luzius Mader (éds.), Öffentlichkeitsgesetz – Handkommentar, Berne 2008, pp. 126 ss.

DÉPARTEMENT FÉDÉRAL DE JUSTICE ET POLICE (DFJP), Pour une administration publique plus transparente, projet de loi fédérale sur la transparence de l'administration et rapport explicatif, Berne avril 2000 (cité : DFJP, Rapport explicatif).

FANTI SÉBASTIEN, La notion de document officiel en droit fédéral, ainsi qu'en droit valaisan, *in* : RVJ 2016, pp. 1-31.

FLÜCKIGER, ALEXANDRE, Commentaire de l'art. 9 LTrans, *in* : Stephan C. Brunner/Luzius Mader (éds.), Öffentlichkeitsgesetz – Handkommentar, Berne 2008, pp. 185 ss.

FLÜCKIGER ALEXANDRE/HÄNNI DOMINIQUE, La transparence en matière d'activités accessoires dans les hautes écoles en Suisse, Genève 2013.

MAHON PASCAL/GONIN OLIVIER, Commentaire des art. 6 et 8 LTrans, *in* : Stephan C. Brunner/Luzius Mader (éds.), Öffentlichkeitsgesetz – Handkommentar, Berne 2008, pp. 106 ss et 165 ss.

OFFICE FÉDÉRAL DE LA JUSTICE (OFJ), Ordonnance relative à la loi fédérale sur le principe de la transparence. Commentaire du 24 mai 2006 (cité : Commentaire OTrans).

OFFICE FÉDÉRAL DE LA JUSTICE (OFJ)/PRÉPOSÉ FÉDÉRAL À LA PROTECTION DES DONNÉES ET À LA TRANSPARENCE (PFPDT), Mise en œuvre du principe de transparence dans l'administration fédérale : questions fréquemment posées (cité : PFPDT, FAQ).

PRÉPOSÉ FÉDÉRAL À LA PROTECTION DES DONNÉES ET À LA TRANSPARENCE (PFPDT), Recommandations, disponibles en ligne sur : https://www.edoeb.admin.ch/oeffentlichkeitsprinzip/00889/01332/index.html?lang=fr.

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

SÄGESSER, THOMAS, Commentaire de l'art. 2 LTrans, *in* : Stephan C. Brunner/Luzius Mader (éds.), Öffentlichkeitsgesetz – Handkommentar, Berne 2008, pp. 32 ss.

SCHÄFER MARC FRÉDÉRIC, Wer entscheidet über den Zugang zu amtlichen Dokumenten, *in* : Jusletter 6 septembre 2010.

SCHEFER MARKUS, Öffentlichkeit und Geheimhaltung in der Verwaltung, *in* : Astrid Epiney/Patrick Hobi (éds.), La révision de la loi sur la protection des données, Zurich 2009, pp. 67-98.

SCHOCH FRIEDRICH, Informationsfreiheitsgesetz – Kommentar, 2e édition, München 2016.

SCHWEIZER, RAINER J./WIDMER NINA, Commentaire de l'art. 3 LTrans, *in* : Stephan C. Brunner/Luzius Mader (éds.), Öffentlichkeitsgesetz – Handkommentar, Berne 2008, pp. 51 ss.

WALTER JEAN-PHILIPPE, Le droit à l'oubli : la perspective européenne, *in* : Tristan Gianora (éd.), Le droit à l'oubli : du mythe à la réalité, Lausanne 2015, pp. 5-22.

DEUXIEME PARTIE

Questions spécifiques

VINCENT CARRON et CATHERINE WENIGER

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

Sommaire

		Page
I.	Introduction	112
II.	La protection des données personnelles des employés	112
	A. Base légale	112
	B. Principes généraux	113
III.	Transferts d'entreprises	115
	A. Transfert des relations de travail des employés	115
	B. Information et consultation des employés	117
	C. Etapes usuelles d'un transfert d'entreprise	119
	1. Discussions préalables	119
	2. Due diligence	120
	3. Signature du contrat	122
	4. Closing et mise en oeuvre	122
IV.	Transmission des données des employés au potentiel acquéreur avant le transfert des relations de travail	123
	A. Formes des données	123
	1. Les données anonymes	123
	2. Les données reconnaissables	124
	3. Les données nominales	125
	B. Illicéité de principe ?	125
	1. Le cadre de l'article 328b CO	125
	2. Relation entre l'article 328b CO et la LPD	127
	C. Motifs justificatifs	128
	1. La loi	128
	2. Le consentement de l'employé	130
	3. Un intérêt prépondérant privé ou public	134
V.	Transmission des données des employés après le transfert de l'entreprise	136
VI.	Conclusion	137
Bibliographie		137

I. Introduction

Traditionnellement, les fusions et acquisitions étaient le monopole des avocats « *corporate* », les aspects de droit du travail et de protection de données étant parfois largement sous-estimés, voire négligés. Cette situation est bien révolue et les transactions sont fréquemment abordées sur deux fronts en parallèle (équipes d'*employment lawyers* d'une part et de *corporate lawyers* d'autre part, tant pour l'acquéreur que le vendeur), avec souvent, dans les transactions multi-juridictionnelles, des canaux de communication bien distincts.

La présente contribution porte sur le traitement de données d'employés dans le cadre de transferts d'entreprises au sens de l'art. 333 CO (rappelant que cet article s'applique également en cas de fusion et de scission). Ce traitement met en œuvre des problématiques liées au droit de la protection des données, mais également liées au droit du travail.

II. La protection des données personnelles des employés

A. Base légale

La protection des données est une composante de la protection de la personnalité garantie à l'article 28 du Code civil[1]. Les articles 328ss du Code suisse des Obligations (CO) régissent plus spécifiquement la protection de la personnalité des travailleurs dans leurs relations avec leur employeur.

La protection particulière des données personnelles fait l'objet de la loi fédérale du 19 juin 1992 sur la protection des données (LPD), en vigueur depuis le 1er juillet 1993.

Le chiffre 2 de l'annexe à la LPD a introduit l'article 328b CO, consacré à la protection de la personnalité lors du traitement de données personnelles des travailleurs par leur employeur. Selon le message du Conseil fédéral, cet article est destiné à compléter la LPD pour accorder une protection particulière aux travailleurs, principalement en déterminant la nature des informations qu'un employeur peut traiter sur ses employés[2]. Pour le surplus, cet article 328b CO renvoie aux dispositions de la LPD.

La LPD énonce des dispositions générales de protection des données, pose les règles sur le traitement des données personnelles par des personnes privées et par des organes

[1] MAURER-LAMBROU/KUNZ, N 7 ss *ad* art. 1 LPD et N 1-8 *ad* art. 12 LPD ; FEY, N 17-19 *ad* art. 1 LPD.
[2] Message LPD, FF 1988 II 421 (494) ; MEIER, Protection des données, N 324 ss, pp. 169 ss.

fédéraux, institue un Préposé fédéral à la protection des données et prévoit des sanctions pénales en cas de violation de ses dispositions.

Le Préposé fédéral à la protection des données (PFPDT), qui est nommé par le Conseil fédéral avec l'approbation de l'Assemblée fédérale[3], a publié de nombreux guides et communications. On peut citer parmi ces textes le « Guide pour le traitement des données personnelles dans le secteur du travail », ainsi que la communication sur la « Transmission de données lors de concentrations d'entreprises »[4]. Il convient de relever que les guides et communications du Préposé fédéral n'ont pas force de loi. Ils expriment néanmoins la position et les standards requis par l'autorité chargée de surveiller l'application de la LPD et de toutes dispositions de droit fédéral relatives à la protection des données[5]. En ce sens, un traitement de données qui respecte les prises de position du Préposé fédéral bénéficiera d'un *a priori* favorable quant à sa licéité, et vice-versa.

B. Principes généraux

Selon les termes de l'article 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* ». Cet article renvoie pour le surplus aux dispositions de la LPD.

L'article 3 LPD définit les notions de *données personnelles* et de *traitement* de données de façon très large. Sont des *données personnelles* toutes les informations qui se rapportent à une personne identifiée ou identifiable[6]. Quant au *traitement* de données, ce terme englobe toutes les opérations relatives à des données personnelles, notamment la collecte, la conservation, l'exploitation, la modification, la communication, l'archivage et la destruction de données[7].

Tout traitement de données personnelles doit respecter certains principes fondamentaux, qui sont énoncés aux articles 4, 5 alinéa 1 et 7 alinéa 1 LPD :

– Le traitement ne doit pas contrevenir à une norme légale destinée à protéger la personnalité de la personne concernée (principe de licéité)[8].

---

3 Art. 26 al. 1 LPD.

4 Disponibles sur le site internet du Préposé fédéral https://www.edoeb.admin.ch/datenschutz/00628/index.html?lang=fr.

5 Art. 27 al. 1 LPD ; MEIER, Protection des données, N 268 ss, p. 142.

6 Art. 3 lit. a LPD.

7 Art. 3 lit. e LPD.

8 Art. 4 al. 1 LPD ; BAERISWYL, N 9-135 *ad* art. 4 LPD.

– Il doit être exécuté conformément aux principes de la bonne foi et de la proportionnalité[9]. Le principe de proportionnalité exige lui-même le respect de différents éléments ou sous-principes. Il exige que le traitement de données réponde :
  - à un besoin effectif
  - pour atteindre un but légitime
  - et soit limité aux seules données nécessaires pour atteindre le but légitime visé[10].
– Les données ne doivent être traitées que dans le but qui est indiqué lors de leur collecte, qui est prévu par une loi ou qui ressort des circonstances (principe de finalité)[11].
– La collecte de données et le but de cette collecte doivent être reconnaissables pour la personne concernée (principe de reconnaissabilité)[12].
– La personne qui traite des données doit s'assurer qu'elles sont correctes (principe d'exactitude)[13].
– Les données doivent être protégées contre tout traitement non autorisé par des mesures organisationnelles et techniques appropriées (principe de sécurité)[14].

L'article 12 alinéa 1 LPD pose la règle de principe selon laquelle le traitement de données ne doit pas constituer une atteinte illicite à la personnalité de la personne concernée. À son alinéa 2, cet article dresse une liste non exhaustive de cas dans lesquels le traitement est réputé porter une atteinte illicite à la personnalité[15].

Selon la lettre a de l'article 12 alinéa 2 LPD, tout traitement de données exécuté en violation de l'un des principes fondamentaux de licéité, de bonne foi et de proportionnalité, de finalité, de reconnaissabilité, d'exactitude ou de sécurité est interdit. Un traitement de données qui ne respecte pas l'ensemble des principes énoncés aux articles 4, 5 alinéa 1 et 7 alinéa 1 LPD constitue une atteinte illicite à la personnalité des personnes concernées[16].

Les chiffres b et c de l'article 12 alinéa 2 LPD interdisent quant à eux le traitement de données contre la volonté expresse de la personne concernée et la communication à des

9 Art. 4 al. 2 LPD.
10 MEIER, Protection des données, N 661-688, pp. 267 ss ; BAERISWYL, N 20-25 *ad* art. 4 LPD ; MAURER-LAMBROU/STEINER, N 9-12 *ad* art. 4 LPD.
11 Art. 4 al. 3 LPD.
12 Art. 4 al. 4 LPD.
13 Art. 5 al. 1 LPD.
14 Art. 7 al. 1 LPD.
15 RAMPINI, N 2-3 *ad* art. 12 LPD.
16 WERMELINGER, N 4 *ad* art. 12 LPD ; RAMPINI, N 8-9 *ad* art. 12 LPD.

tiers de données sensibles ou de profils de la personnalité, sauf s'il existe un motif justificatif.

Il faut préciser ici que l'illicéité de principe d'un traitement qui viole l'un des principes énoncés aux articles 4, 5 alinéa 1 et 7 alinéa 1 LPD peut également être levée en présence d'un motif justificatif. En effet, même si le texte de l'article 12 alinéa 2 lettre a LPD ne réserve pas l'existence d'un motif justificatif, le Tribunal fédéral a précisé que, malgré sa lettre, l'article 12 alinéa 2 lettre a LPD permet bien les motifs justificatifs (comme dans les lettres b et c) mais que ceux-ci ne peuvent être admis qu'avec une grande retenue[17]. Un traitement de données personnelles qui viole un ou plusieurs des principes de licéité, de bonne foi et de proportionnalité, de finalité, de reconnaissabilité, d'exactitude ou de sécurité peut ainsi être autorisé en présence d'un des motifs justificatifs reconnus par la loi.

L'article 13 alinéa 1 LPD énonce les motifs justificatifs qui lèvent l'illicéité de principe d'une atteinte à la personnalité de la personne concernée[18]. Selon le texte de cette disposition, toute atteinte est illicite sauf si elle est justifiée par le consentement de la victime, par un intérêt prépondérant privé ou public, ou par la loi.

III. Transferts d'entreprises

Un transfert d'entreprise peut revêtir plusieurs formes juridiques. Il peut s'agir d'une fusion, par absorption ou par combinaison, entre deux ou plusieurs entités, d'une scission, par division ou par séparation, du patrimoine d'une entité vers une ou plusieurs autres entités ou d'un transfert de patrimoine. Il peut s'agir d'un simple transfert conventionnel d'actifs. Une entreprise peut aussi être transférée par la cession de son actionnariat (*share deal*).

A. Transfert des relations de travail des employés

L'article 333 alinéa 1 CO indique que si l'employeur transfère l'entreprise ou une partie de celle-ci à un tiers, les rapports de travail passent à l'acquéreur avec tous les droits et les obligations qui en découlent, au jour du transfert, à moins que le travailleur ne s'y oppose.

Dans ce cadre, est considéré comme un « *transfert d'entreprise* » tout transfert d'une unité de production organisée formant un tout, prévue pour durer, qui participe de manière

[17] ATF 136 II 508 = JdT 2011 II 446, c. 5 et 6.3 ; WERMELINGER, N 5 *ad* art. 12 LPD ; RAMPINI, N 9b *ad* art. 12 LPD.

[18] WERMELINGER, N 3 *ad* art. 12 LPD.

indépendante à la vie économique. Sont aussi visés par l'article 333 CO les transferts de parties d'entreprise, c'est-à-dire d'unités de production organisées, qui sont dépourvues d'indépendance économique. Il faut néanmoins toujours que l'entité organisée conserve pour l'essentiel son identité, à savoir le but social, l'organisation et le caractère individuel[19].

La Loi fédérale sur la fusion, la scission, la transformation et le transfert de patrimoine (LFus) prévoit expressément l'application de l'art. 333 CO en cas de fusion (art. 27 LFus), scission (art. 49 LFus) et transfert de patrimoine (art. 76 LFus).

Le champ d'application de l'art. 333 CO est large, et le Tribunal fédéral a eu l'occasion de juger qu'il ne supposait même pas forcément une relation juridique entre le précédent et le nouvel exploitant[20].

L'art. 333 CO ne concerne cependant pas les cessions d'actionnariat (*share deals*). Ceux-ci n'impliquent en effet pas de changement d'employeur.

L'art. 333 CO est relativement impératif. Il ne peut donc pas y être dérogé conventionnellement en défaveur du travailleur[21].

De même, l'employeur qui transfère l'entreprise et celui qui la reprend ne peuvent pas conclure d'accord dérogatoire. Ni le vendeur ni l'acquéreur ne peuvent déterminer quels contrats de travail vont passer (automatiquement) à l'acquéreur ou non, dans la mesure où les employés concernés sont bien rattachés, au moment du transfert, à l'entreprise ou partie d'entreprise concernée. Il s'agit là d'une opération de la loi.

Chaque employé concerné a néanmoins le droit de s'opposer à son transfert. En cas d'opposition d'un employé, les rapports de travail prennent fin à l'expiration du délai de congé légal mais au plus tôt au jour du transfert. Si le délai de congé légal n'est pas échu au jour du transfert, les rapports de travail passent à la nouvelle entité au moment du transfert, pour prendre ensuite définitivement fin à l'expiration du délai de congé légal[22].

Lors d'un transfert d'entreprise au sens de l'art. 333 CO, les employés sont ainsi automatiquement transférés à l'acquéreur, qui devient leur nouvel employeur, le jour où le transfert d'entreprise prend effet. Le contrat de travail de chaque employé est de par la loi repris par le nouvel employeur dans ses termes et conditions au jour du transfert

---

19 ATF 129 III 335 = JdT 2003 II 75 ; WYLER/HEINZER, pp. 448 ss.

20 ATF 123 III 466. Critiques à juste titre selon nous : STREIFF/VON KAENEL/RUDOLPH, N 5 *ad* art. 333 CO.

21 Art. 362 CO.

22 WYLER/HEINZER, pp. 462-463 ; STREIFF/VON KAENEL/RUDOLPH, N 12 *ad* art. 333 CO ; CHENAUX/MARTIN, N 20 *ad* art. 333 CO.

d'entreprise. Le nouvel employeur est tenu de respecter tous les droits et obligations résultant des rapports de travail tels qu'ils existent au jour de leur transfert.

Si le nouvel employeur entend modifier les conditions contractuelles d'emploi, il doit soit obtenir de chaque employé qu'il signe un avenant à son contrat de travail ou un nouveau contrat, soit procéder par la voie d'un congé-modification[23]. Si les relations de travail transférées sont régies par une convention collective, l'acquéreur est cependant tenu de la respecter durant une année, sous réserve qu'elle prenne fin par l'expiration de sa durée convenue ou par sa dénonciation.

B. Information et consultation des employés

Au vu du transfert des relations de travail résultant de l'art. 333 CO, l'article 333a alinéa 1 CO impose à l'employeur qui transfère son entreprise ou une partie de celle-ci à un tiers d'informer la représentation des travailleurs ou, à défaut, les travailleurs en temps utile avant la réalisation du transfert de l'entreprise sur le motif du transfert ainsi que sur les conséquences juridiques, économiques et sociales du transfert pour les travailleurs.

L'alinéa 2 de cette disposition exige en outre la consultation de la représentation des travailleurs ou, à défaut, des travailleurs si des mesures concernant les travailleurs sont envisagées suite au transfert de l'entreprise. Cette consultation doit avoir lieu en temps utile avant que ces mesures ne soient décidées.

L'employeur a ainsi l'obligation d'informer la représentation des travailleurs, ou à défaut les employés, sur les conséquences que la transaction aura pour eux et de les consulter si des mesures les concernant sont envisagées. Des auteurs évoquent par exemple les conséquences suivantes :

- des licenciements (si le seuil d'un licenciement collectif au sens de l'article 335d CO risque d'être atteint, la procédure des articles 335d à 335f CO doit en outre être respectée) ;
- une restructuration de l'entreprise de l'acquéreur après le transfert ;
- des modifications des droits et des obligations contractuels des employés ou simplement de leur conditions effectives de travail, par exemple, un changement du lieu de travail, des modifications dans la rémunération (salaire, bonus, plans d'intéressement), la suppression ou la modification d'assurances en faveur des

[23] Si les seuils d'un licenciement collectif au sens de l'article 335d CO sont atteints, les congé-modifications devront être précédés d'une consultation des employés conforme à l'art. 335f CO et la procédure de l'art. 335g CO devra être respectée. Nous n'examinons pas ici la question de la licéité d'un congé-modification effectué pour la date du transfert.

employés (par exemple, assurance accident complémentaire, assurance perte de gain, assurance voyage)[24].

Selon le texte de l'article 333a CO le devoir d'informer et de consulter incombe à l'employeur. D'un point de vue pratique, les conséquences du transfert et les modifications envisagées dépendent essentiellement des projets de l'acquéreur. De nombreux auteurs considèrent dès lors que, compte tenu de l'implication nécessaire de l'acquéreur dans l'information et la consultation des employés de l'entreprise-cible, vendeur et acquéreur de l'entreprise forment une communauté d'employeurs dans ce cadre et sont tous deux soumis aux obligations de l'article 333a CO[25].

Dans le cadre d'une transaction régie par la LFus, la consultation de la représentation des travailleurs est également régie par l'article 333a CO par renvoi de la loi à cette disposition. La LFus impose en outre que tant la société transférante que la société reprenante respecte les obligations découlant de l'article 333a CO envers ses propres employés[26]. La violation des obligations d'information et de consultation de l'article 333a CO, dans la société transférante ou dans la société reprenante, ouvre le droit pour la représentation des travailleurs d'exiger du juge qu'il interdise l'inscription de la fusion, de la scission ou du transfert de patrimoine au registre du commerce[27].

Alors que l'article 333a alinéa 2 CO indique simplement que la consultation doit avoir lieu en temps utile avant que ces mesures ne soient décidées, l'article 28 alinéa 2 LFus impose, en cas de fusion ou de scission, que la consultation ait lieu avant que la transaction soit approuvée par les entités concernées conformément à l'article 18 LFus. L'organe supérieur de direction ou d'administration doit informer l'assemblée générale du résultat de la consultation lors de la décision[28].

---

24 Nous ne prenons pas ici position sur la question du niveau de détail requis lors d'une consultation, ni sur la définition de ce qui doit être considéré (à partir de quel niveau d'intensité) comme des « mesures » envisagées imposant la tenue d'une consultation, ou encore comme des « conséquences juridiques, économiques ou sociales » faisant partie du devoir d'information.

25 WYLER/HEINZER, p. 458 ; CHENAUX/MARTIN, N 4 *ad* art. 333a CO ; STREIFF/VON KAENEL/RUDOLF, N 6 *ad* art. 333a CO.

26 Cf. art. 28 al. 1 LFus en cas de fusion, art. 50 LFus en cas de scission et art. 77 al. 1 LFus en cas de transfert de patrimoine.

27 Cf. art. 28 al. 3 LFus en cas de fusion, art. 50 LFus en cas de scission et art. 77 al. 2 LFus en cas de transfert de patrimoine.

28 Art. 28 al. 2 LFus, auquel renvoie aussi l'art. 50 LFus en cas de scission. Pour plus de détails, et notamment en cas de fusion simplifiée, cf. WYLER/HEINZER, pp. 474 ss.

C. Etapes usuelles d'un transfert d'entreprise

Un projet de transfert d'entreprise traverse usuellement plusieurs étapes au cours desquelles les parties échangent de nombreuses informations. Nous décrivons ici les principales phases qui peuvent être rencontrées dans un transfert d'entreprise soumis à l'art. 333 CO.

1. Discussions préalables

Dans cette phase initiale, l'entité intéressée à vendre ou transférer une entreprise ou une partie de celle-ci, peut entrer en contact avec une ou plusieurs autres entités susceptibles d'être intéressées au projet. L'objectif des discussions est de déterminer un candidat sérieux avec lequel la poursuite du projet pourrait aboutir à la conclusion de l'opération.

À ce stade, les informations échangées demeurent très générales. L'information principale que communique l'entité à l'origine du projet est qu'elle envisage une fusion ou un transfert d'entreprise, ainsi que les grandes lignes du projet qu'elle conçoit. Seules des informations générales sur l'entreprise à vendre et des données financières globales sont communiquées. Elles sont transmises soit pour évaluer l'entreprise à céder soit pour vérifier une évaluation déjà faite par le vendeur potentiel. Aucune donnée personnelle concernant les employés n'est usuellement transmise dans le cadre de ces négociations préalables.

Dans certains projets où plusieurs entités se sont déclarées intéressées (ce peut être notamment le cas lorsque le vendeur potentiel a directement approché diverses acheteurs potentiels – *auction process)*, le vendeur potentiel met à leur disposition des informations plus étendues sur sa situation financière et sur la marche de ses affaires. L'objectif est de permettre aux entités intéressées de faire un première évaluation et de déterminer si et à quelles conditions elles souhaitent poursuivre le projet de transaction. Des données générales sur les finances et les opérations de l'entreprise-cible suffisent généralement pour une telle évaluation.

Il est en outre d'usage que les parties signent des accords de confidentialité au début des discussions ou au cours de celles-ci. Ces accords lient tous les organes et employés impliqués dans la conduite du projet dans chacune des entités.

Cette phase de discussions se termine lorsque le cercle des partenaires possibles au projet a été restreint à une entité ayant manifesté un intérêt sérieux. Se trouvent alors en présence, d'une part, l'entité à l'origine du projet et, d'autre part, le cocontractant potentiel. Dans le cadre d'un *auction process*, plus qu'une seule partie intéressée pourra toutefois rester en piste à ce stade.

Souvent, après les premières discussions entre l'entité à l'origine du projet et le cocontractant potentiel, une lettre d'intention est signée qui définit les grandes lignes de la transaction envisagée[29]. Cette lettre d'intention peut être une pure déclaration d'intention sans force obligatoire ou déjà constituer un contrat générateur de droits et d'obligations pour les parties.

Dans tous les cas, la conclusion d'un contrat de fusion ou de transfert demeure soumise à de nombreuses conditions préalables, parmi lesquelles figure la communication d'informations complémentaires sur l'enteprise-cible et le résultat de l'analyse de ces informations par l'entité-reprenante. À ce stade, l'aboutissement de la fusion ou du transfert d'entreprise projeté demeure très incertain.

2. Due diligence

Le cocontractant potentiel demande dans la plupart des cas à procéder à une vérification de la situation de l'entité qu'il se propose d'acquérir. Il s'agit d'une procédure préalable à la signature d'un contrat de fusion ou de transfert d'entreprise. L'objectif du cocontractant potentiel est d'évaluer la situation globale de l'entreprise-cible sous les angles commercial, juridique, fiscal et financier. Cette évaluation est couramment désignée sous l'appellation « due diligence ».

Parmi les informations pertinentes pour le cocontractant potentiel, les données sur le personnel de l'entreprise-cible sont particulièrement importantes[30].

En effet, la masse salariale, tous types de rémunérations confondus, et les coûts liés au personnel, tels que les charges sociales et les cotisations de prévoyance professionnelle, de même que les prétentions litigieuses d'employés, peuvent avoir une influence considérable sur les résultats de l'entreprise. Savoir si des employés ont droit à des indemnités en cas de changement dans la personne de l'employeur ou dans l'actionnariat de la société employeur, et le montant de ces indemnités, est également une information pertinente pour évaluer les coûts et profits potentiels du projet. Connaître l'organigramme du personnel et les tâches de chaque employé est nécessaire à l'entité intéressée pour repérer d'éventuels sous-effectifs ou surcapacités dans certains services ou profils. D'une façon générale, le cocontractant potentiel a un intérêt à connaître tous les détails des conditions d'emploi des employés de l'entreprise-cible afin de déterminer les possibilités et les coûts d'une éventuelle restructuration postérieure au transfert, qui peut parfois être indispensable suivant le projet envisagé.

---

[29] Ce document est généralement désigné sous le nom de « *letter of intent* », « *memorandum of understanding* » ou « *term sheet* ».

[30] MEIER, *Due diligence*, p. 191.

Définir qui sont les employés essentiels (*key employees*) à la bonne marche des affaires et quelles sont leurs conditions d'emploi (salaire, bonus, plans de participation, délai de congé, engagement de non-concurrence, indemnités de départ, existence de *retention agreements*) est également important pour l'acquéreur potentiel. Celui-ci doit pouvoir déterminer les mesures utiles pour s'assurer la collaboration de ces employés après la transaction, respectivement évaluer les risques pour la société s'ils devaient la quitter.

L'acquéreur potentiel a également un intérêt manifeste à connaître les assurances conclues en faveur des employés (assurance accident complémentaire, assurance perte de gain, etc.). Outre les coûts que ces assurances génèrent, leur compatibilité avec celles en vigueur au sein de l'entité-reprenante, respectivement les conditions des polices d'assurance que celle-ci devrait conclure pour répliquer les conditions actuelles, sont des informations importantes pour l'évaluation du projet de fusion ou de transfert. Dans le même sens, l'existence d'une convention collective applicable aux relations de travail et ses termes doivent également être connus de l'acquéreur potentiel avant sa prise de décision sur la transaction envisagée.

On comprend de cette liste non exhaustive des informations sur les employés qui sont nécessaires au cocontractant potentiel pour évaluer la situation financière actuelle et future de l'entreprise-cible et les risques légaux potentiels du projet de fusion ou de transfert que cette phase du processus cristallise le conflit entre les intérêts de l'acquéreur potentiel, et aussi de l'employeur actuel qui souhaite que le projet se réalise d'une part, et la protection des données personnelles des employés d'autre part.

Le niveau de détail des informations sur les employés que requiert le cocontractant peut varier d'un projet à l'autre, notamment en fonction de la taille des entreprises concernée.

Il n'est pas rare que la liste nominative des employés concernés avec leurs fonctions dans l'entreprise soit requise et communiquée. Une liste nominative distincte des employés dont le salaire excède une certaine somme et/ou qui bénéficient de droits contractuels particulièrement étendus est également une pratique courante.

Enfin, les données détaillées des employés qui disposent d'une connaissance complète des affaires de l'entreprise-cible ou de la partie de l'entreprise dont le transfert est envisagé et/ou qui entretiennent les relations avec les clients et fournisseurs de celle-ci et/ou sont des éléments importants de son succès (*key employees*) sont souvent considérées comme des informations essentielles pour le cocontractant potentiel et font l'objet d'une communication.

Toutefois, le niveau d'information que l'acquéreur potentiel obtiendra du vendeur en pratique, dans le cadre de la due diligence, pourra aussi considérablement dépendre de la sensibilité de ce dernier et/ou de ses conseils aux questions de protection des données.

Il est devenu désormais de plus en fréquent que des vendeurs potentiels refusent de remettre à ce stade toute liste de noms d'employés (sous réserve parfois de celle des *key employees*), et ne remettent pas de contrats de travail individualisés. Ils tendent à ne rendre accessibles, durant la due diligence, que des modèles de contrats utilisés par type d'employés (contrat pour employés non-cadres; contrats pour employés-cadres, etc.).

3. Signature du contrat

Cette étape correspond à la signature du contrat de fusion ou d'acquisition de l'entreprise. À ce stade, les parties se lient contractuellement et leurs droits et devoirs réciproques sont fixés.

Dans la pratique des transactions, le contrat comporte souvent de nombreuses annexes. Parmi ces annexes figurent les listes des actifs, mobiliers et immobiliers, des contrats, des droits et des obligations qui sont cédés dans le cadre de la transaction. La liste des employés dont la relation de travail sera transférée à l'acquéreur fait également partie des annexes habituelles d'un contrat de fusion ou de transfert d'entreprise.

Il est cependant courant que l'exécution du contrat, à savoir l'entrée en force de la fusion ou du transfert d'entreprise, soit arrêtée à une date bien ultérieure. Le contrat peut notamment exiger que l'une ou l'autre des parties, voire les deux, exécute certaines actions ou réalise certaines conditions préalablement à l'entrée en vigueur de la transaction. La transaction doit parfois obligatoirement être soumise à des autorités administratives et obtenir leur aval avant d'être exécutée. On pense notamment à la loi sur les cartels (LCart) qui exige que les opérations de concentration d'entreprises d'une certaine ampleur soient notifiées avant leur réalisation à la Commission de la concurrence, qui peut cas échéant les interdire ou imposer des conditions.

Lorsque la signature du contrat ne coïncide pas avec l'entrée en force du transfert d'entreprise, l'acquéreur demeure un tiers vis-à-vis des employés du vendeur. Il n'existe aucune relation contractuelle entre eux. Le risque que le contrat ne soit finalement pas exécuté demeure, à des degrés divers suivant les cas particuliers, et il n'est pas encore absolument certain que l'acquéreur devienne dans un avenir plus ou moins proche l'employeur des employés de l'entreprise-cible.

4. Closing et mise en oeuvre

Il s'agit de la phase finale qui débute le jour de l'exécution du contrat[31]. Elle se poursuit jusqu'à ce que toutes les créances et les obligations en relation avec le contrat de fusion ou d'acquisition de l'entreprise soient exécutées.

[31] La date de l'exécution du contrat est couramment désignée sous son appellation anglophone « *Closing* » ou « *Closing Date* ».

C'est uniquement à ce stade, soit au jour de l'exécution du contrat de fusion ou de transfert, que l'acquéreur devient l'employeur des employés de l'entreprise-cible.

IV. Transmission des données des employés au potentiel acquéreur avant le transfert des relations de travail

L'intérêt du tiers qui se propose d'acquérir l'entreprise de l'employeur, par le biais d'une fusion ou d'une acquisition, à disposer d'informations sur les employés de l'entreprise-cible et sur les modalités de chaque relation de travail a été relevé ci-dessus.

Se pose dès lors la question de savoir si l'entreprise-cible peut, en sa qualité d'employeur, fournir à son cocontractant potentiel des données concernant ses employés, lesquelles et à quelles conditions.

A. Formes des données

1. Les données anonymes

Il faut rappeler que les dispositions sur la protection des données, qu'il s'agisse de la LPD ou de l'article 328b CO, ne s'appliquent qu'aux traitements de données personnelles au sens de l'article 3 lettre a LPD. Les informations qui ne se rapportent pas à une personne identifiée ou identifiable ne sont pas des données personnelles au sens de la loi et leur traitement n'est pas soumis aux dispositions légales sur la protection des données[32].

Dans le cadre d'un projet de fusion ou de transfert d'entreprise, l'entreprise-cible peut donc fournir à l'acquéreur potentiel toute information qui ne peut pas être reliée à une ou des personnes identifiées[33].

En principe, toutes les informations sur les employés et leurs conditions de travail devraient ainsi pouvoir être transmises au cocontractant potentiel sur une base anonyme. Dans la mesure où les données anonymes transmises ne permettent pas de faire le lien avec une personne déterminée ou déterminable les dispositions sur la protection des données ne sont pas applicables.

---

32 RUDIN, N 3-10 *ad* art. 3 LPD ; BLECHTA, N 3-13 *ad* art. 3 LPD ; MEIER, Protection des données, N 438, p. 204.

33 MAURER-LAMBROU/STEINER, N 19 *ad* art. 4 LPD.

2. Les données reconnaissables

Le caviardage d'informations sur les employés est une solution couramment utilisée dans la pratique des transactions. Ainsi, par exemple, les contrats de travail, avec leurs éventuels annexes et avenants, et le montant de la rémunération actuelle peuvent être remis sans qu'apparaisse l'identité du collaborateur concerné (un numéro remplaçant le nom et l'adresse de l'employé). L'acquéreur potentiel reçoit également les conditions générales d'emploi (polices d'assurance, règlement du personnel, plans de pension, plans de participation, etc.). L'acquéreur potentiel dispose ainsi de toutes les informations utiles, seule l'identité des employés n'étant pas divulguée.

Il peut toutefois arriver que des informations a priori anonymes puissent être reliées à une personne déterminée, malgré la suppression de l'identité de celle-ci, grâce à d'autres informations dont le cocontractant est susceptible de prendre connaissance.

On pense par exemple au registre du commerce qui indique les noms et fonctions des personnes autorisées à engager la société par leur signature ou au site internet de l'employeur qui peut contenir l'organigramme nominatif du personnel, à tous le moins des cadres. Le nom et la fonction des cadres supérieurs d'une entreprise sont en outre souvent connus des acteurs opérants dans le même milieu économique, voire du public suivant l'importance de la société.

En rapprochant ces informations publiques avec les données transmises par l'entreprise-cible, le lien peut dans certains cas être fait avec une personne déterminée. Si les données transmises indiquent le titre et la fonction de chaque employé, il sera dans bien des cas faciles à l'acquéreur potentiel de relier certains contrats de travail à des personnes déterminées. Par exemple, le contrat de travail du « directeur général » pourra être attribué à M. X si celui-ci est la seule personne inscrite au registre du commerce avec le titre de directeur ou s'il est de notoriété publique que M. X est le directeur général de l'entreprise-cible.

Même en l'absence d'information publique, l'acquéreur pourrait découvrir l'identité du collaborateur concerné par certaines données, remises sous forme anonyme, par ses contacts au sein de l'entreprise-cible au cours des négociations. Il arrive en effet fréquemment en pratique, principalement lorsque le projet est déjà avancé, que des contacts directs aient lieu entre l'acquéreur potentiel et des employés de l'entreprise-cible sur certains aspects de la transaction. On pense par exemple aux responsables financiers sur les questions de comptabilité, aux responsables produits sur les questions de développement ou aux responsables des ressources humaines sur les questions liées au personnel. L'acquéreur potentiel prend ainsi connaissance du nom et de la fonction de ces collaborateurs de l'entreprise-cible. S'il dispose de données qui font référence au poste du collaborateur concerné, il pourra sans difficulté les relier à l'individu avec lequel il aura eu un contact.

Le seul moyen d'éviter ce risque est de caviarder toutes les indications qui, combinées à d'autres informations, seraient susceptibles de permettre que les données soient être reliées à une personne identifiée. Cela implique de cacher non seulement le nom et de l'adresse du collaborateur concerné mais aussi, entre autres, sa fonction, le titre de son supérieur hiérarchique, certains passages de clauses de non-concurrence qui décrivent les secrets auxquels l'employé a accès, la date d'entrée en service, etc. La liste des informations susceptibles de conduire à l'identification d'un employé est cependant tellement vaste, compte tenu des tous les aléas possibles, que même un employeur particulièrement soucieux de la protection des données de ses employés pourrait laisser passer un élément qui pourrait permettre à un cocontractant potentiel particulièrement curieux et motivé de faire le lien avec un individu.

Enfin, si l'acquéreur potentiel ne dispose que de données globales anonymes, il sera souvent dans l'impossibilité de définir le détail des conséquences du transfert pour les travailleurs et des changements dans les modalités d'emploi qui pourraient devoir être mis en œuvre après le transfert.

Lorsque, malgré, leur anonymisation partielle, les données peuvent néanmoins permettre l'identification de certains employés, elles doivent être reconnues comme des données personnelles au sens de la LPD. Leur transfert à un acquéreur potentiel correspond à un traitement de données des employés régis par l'article 328b CO et les dispositions de la LPD auxquelles cet article renvoie.

3. Les données nominales

On entend par données nominales les informations qui permettent immédiatement d'identifier la personne à laquelle les données se réfèrent. Il s'agit par exemple des contrats de travail ou des certificats de salaire avec le nom de l'employé.

Ces données sont des données personnelles au sens de la LPD. Leur traitement doit respecter les dispositions légales sur la protection des données.

B. Illicéité de principe ?

La transmission de données personnelles des employés, soit des données reconnaissables ou nominales, par l'employeur à un acquéreur potentiel pose le problème de sa licéité.

1. Le cadre de l'article 328b CO

L'article 328b CO fixe les buts qui peuvent légitimement être poursuivis par un employeur et qui justifient en principe le traitement des données des employés nécessaires à leur réalisation. Si un employeur traite des données personnelles de ses employés dans le but

de s'assurer de leur aptitude à remplir leur emploi ou en vue de l'exécution du contrat de travail, le traitement est présumé licite.

Le Tribunal fédéral a confirmé ce principe en déclarant que les données personnelles couvertes par l'article 328b CO bénéficient de la présomption légale qu'elles ne portent pas atteinte à la personnalité du travailleur. Il a toutefois précisé que le procédé utilisé pour les récolter doit néanmoins, lui aussi, respecter la personnalité des travailleurs, conformément à l'art. 328 CO, et observer les principes généraux du droit, en particulier ceux de la bonne foi et de la proportionnalité[34].

Il faut donc en déduire que tout traitement de données qui ne poursuit pas l'un des buts énumérés à l'article 328b CO ne bénéficie pas d'une présomption de licéité.

La transmission par un employeur de données personnelles de ses employés à un tiers avec lequel une fusion ou un transfert d'entreprise est envisagé n'entre a priori pas strictement dans l'un des buts énumérés à l'article 328b CO.

Cette remise de données à un tiers ne permet en rien à l'employeur d'évaluer l'aptitude des employés à leurs fonctions. Elle n'est pas non plus nécessaire à l'exécution du contrat de travail, à tout le moins tant que le tiers n'est pas devenu l'employeur des travailleurs ou qu'il n'est pas certain qu'il le devienne.

Un auteur, à tout le moins, estime que la transmission des données des employés dans le cadre d'un projet de fusion ou de transfert d'entreprise peut entrer dans le cadre de l'exécution du contrat de travail car elle sert la reprise et donc la poursuite des relations de travail[35]. Cette position paraît faire sens pour autant que la transmission ait lieu à un moment où le transfert des rapports de travail à l'acquéreur est devenu un fait futur certain. Elle constitue en revanche une interprétation extensive de l'article 328b CO tant que l'exécution de la transaction demeure largement incertaine[36].

Un autre auteur estime quant à lui que l'article 328b CO n'est pas violé si la transaction envisagée est indispensable à la sauvegarde des emplois et que la transmission des données respecte les principes de bonne foi et de proportionnalité. Il justifie cette interprétation par la protection des intérêts des employés[37].

La question de savoir si la remise des données personnelles des employés au cocontractant potentiel dans le cadre d'un projet de transfert d'entreprise bénéficie ou non de la

34 ATF 130 II 425, c. 3.3.
35 GERICKE, p. 6 ; GERICKE/BURRI, N 24.36, p. 883.
36 BALZAN, pp. 13-14.
37 MEIER, Due diligence, pp. 191-192.

présomption de licéité de l'article 328b CO n'est pas tranchée à ce jour. Le risque qu'elle constitue une atteinte en principe illicite à la personnalité des employés ne peut être écarté.

2. Relation entre l'article 328b CO et la LPD

En cas d'atteinte illicite à la personnalité, l'article 13 alinéa 1 LDP réserve, comme nous l'avons mentionné précédemment, l'existence de motifs justificatifs. Selon cette disposition, est illicite toute atteinte à la personnalité à moins d'être justifiée par le consentement de la victime, par un intérêt prépondérant privé ou public, ou par la loi.

La portée de l'article 328b CO en regard des dispositions de la LPD est controversée en doctrine. Le point central de la controverse est de savoir si l'article 328b CO interdit le traitement par l'employeur de données qui sortent du cadre qu'il pose, indépendamment de l'existence d'un motif justificatif prévu à l'article 13 LPD[38].

D'un point de vue historique, le Conseil fédéral a exprimé dans son message que, selon l'article 328b CO, seuls sont licites les traitements de données personnelles qui portent sur les aptitudes du travailleur à remplir son emploi ou qui sont nécessaires à l'exécution du contrat de travail et que l'article 328b CO concrétise ainsi le principe général de la proportionnalité dont le respect est exigé par la LPD[39].

Si l'on admet que l'article 328b CO signifie que le traitement de données qui ne poursuit pas un des buts décrits dans cette disposition est contraire au principe de proportionnalité, un tel traitement de données est illicite en application de l'article 12 alinéa 2 lettre a LPD.

Si, comme la lettre de l'article 12 alinéa 2 lettre a LPD le laisse entendre, un traitement de données effectué en violation de l'un des principes fondamentaux, énoncés aux articles 4, 5 alinéa 1 et 7 alinéa 1 LPD, était absolument interdit sans recours possible à des motifs justificatifs, tout traitement de données d'employés hors du cadre de l'article 328b CO serait effectivement exclu en toute hypothèse. Or, nous avons vu que l'illicéité d'un traitement de données peut être levée par les motifs justificatifs de l'article 13 LPD même si l'illicéité découle de la violation de l'un des principes fondamentaux énoncés aux articles 4, 5 alinéa 1 et 7 alinéa 1 LPD[40].

Compte tenu de ce qui précède, si le traitement de données d'employés par l'employeur dans un but qui sort du cadre fixé par l'article 328b CO est certes illicite en principe, cette

---

38 Pour un exposé détaillé des différentes positions dans la doctrine : MEIER, Protection des données, N 2032-2041, pp. 650 ss.

39 Message LPD, FF 1988 II 421 (494).

40 Cf. II.B *supra*.

illicéité peut être levée si l'employeur peut se prévaloir d'un motif justificatif réservé par la LPD.

Aussi, à notre sens, un employeur peut traiter des données de ses employés qui ne sont pas nécessaires à l'un des deux buts fixés à l'article 328b CO s'il peut faire valoir un motif justificatif prévu à l'article 13 LPD[41]. Demeure la question de savoir si l'employeur peut se prévaloir de tous les motifs justificatifs prévus par la LPD.

C. Motifs justificatifs

1. La loi

Dans l'hypothèse où la transmission par un employeur de données personnelles de ses employés à un tiers avec lequel un transfert d'entreprise est envisagé n'entrerait pas dans l'un des buts énumérés à l'article 328b CO, une autre disposition légale justifierait-elle cette transmission?

Comme indiqué plus haut, l'article 333a CO oblige l'employeur à informer la représentation des travailleurs, ou, s'il n'en existe pas, les employés, sur toutes les conséquences juridiques, économiques et sociales du transfert pour eux. La représentation des travailleurs, respectivement les employés, doit en outre être consultée si de telles mesures sont envisagées. Il s'agit d'un devoir d'informer et de consulter de façon collective les employés, par l'intermédiaire de leur représentation s'ils en ont élu une[42]. Certains auteurs considèrent en outre que, compte tenu de l'implication nécessaire de l'acquéreur dans l'information et la consultation des employés de l'entreprise-cible, vendeur et acquéreur forment une communauté d'employeurs dans ce cadre et sont tous deux soumis aux obligations de l'article 333a CO[43].

Les conséquences de la transaction envisagées sur les conditions de travail des employés concernés et les éventuels changements dans celles-ci ne peuvent être déterminées qu'en comparant les conditions actuelles et les conditions que l'acquéreur envisage de mettre en place après l'exécution de la transaction. Si l'acquéreur a déjà du personnel propre, il souhaite généralement harmoniser les conditions de travail entre ses employés d'origine et les employés qui transfèrent, ou veiller à ce que les salaires de ses derniers soient cohérents avec l'échelle qu'il utilise. Une telle harmonisation peut d'ailleurs être

41 En ce sens, MEIER, Protection des données, N 2037, pp. 650-651 et les références citées ; BALZAN, p. 6 ; BAUMANN, p. 639 ; arrêt de la Cour de Justice de Genève, ACJC/1529/2015 du 11 décembre 201511.12.2015, not. c. 5.1.2.

42 WYLER/HEINZER, p. 464 ; WILDHABER, pp. 376-377.

43 WYLER/HEINZER, p. 458 ; CHENAUX/MARTIN, N 4 *ad* art. 333a CO.

nécessaire pour respecter la loi sur l'égalité ou éviter des inégalités non justifiables objectivement.

L'acquéreur potentiel ne peut lui-même déterminer si et dans quelles mesures il envisage des changements dans les conditions de travail que s'il connaît les conditions actuelles des employés concernés.

Les obligations légales d'information et de consultation des employés justifient dès lors à notre avis que l'employeur actuel, soit l'entreprise-cible, fournisse à l'acquéreur potentiel les informations sur les conditions et modalités des relations de travail avec les employés concernés dans la mesure utile à l'exercice des obligations d'information et de consultation de l'art. 333a CO.

Dans la mesure où la transmission est faite aux fins d'évaluer la teneur de l'information imposée par l'art. 333a CO et si une consultation doit être tenue, ce traitement de données, qui serait justifié ainsi par l'art. 333a CO, doit donc être accompli avant l'étape de l'information et de la consultation.

On rappelle que l'information, laquelle doit porter aussi sur les conséquences juridiques économiques ou sociales envisagées doit avoir lieu en temps utile avant la réalisation du transfert (art. 333a al. 1 CO). Pour la consultation, il ressort du système qu'elle doit également avoir lieu avant la réalisation du transfert (et bien évidemment avant que les mesures aient été définitivement décidées). Pour les opérations fondées sur la LFus, la situation est claire : la consultation doit dans tous les cas être parfaite avant la décision de fusion (art. 18 LFus)[44], avant la décision de scission (art. 50 LFus), et avant l'inscription du transfert de patrimoine au registre du commerce en cas de transfert de patrimoine soumis à la LFus (art. 77 LFus).

Une période de consultation de deux semaines est généralement suffisante. Toutefois, suivant la taille des entités concernées et l'ampleur des modifications envisagées concernant les travailleurs, la « communauté d'employeurs » pourra décider de prévoir d'emblée une durée plus longue, voire se réserver, dans sa planification interne, une certaine marge, pour accorder une prolongation de délai, en cas de requête en ce sens par la représentation des travailleurs, ou ceux-ci.

Par conséquent, le traitement de l'information nécessaire à la compréhension par l'employeur futur des impacts que pourrait produire le transfert sur les salariés, aura lieu avant la consultation, et, partant, plusieurs semaines avant le transfert et l'acquisition, pour le reprenant, d'une qualité d'employeur.

---

[44] Plus précisément, la prise de décision par l'Assemblée générale. Cf. à ce sujet notamment, WYLER/HEINZER, p. 475.

Il se pose ensuite la question de la qualité des données relatives aux employés qui peuvent être traités aux fins de la consultation, sous l'angle d'une justification donnée par l'art. 333a CO.

La procédure d'information et de consultation prévue par le Code des obligations n'est comprise que comme une procédure de nature collective. L'article 333a CO n'impose pas que l'employeur informe chaque employé individuellement des conséquences et mesures qui pourraient l'affecter sur la base de sa situation personnelle[45]. D'ailleurs, l'interlocuteur primaire de la « communauté des employeurs » est d'abord la représentation des travailleurs et ce n'est qu'à défaut d'existence, que les travailleurs sont informés et consultés, sur une base collective. Des données nominatives ne seront donc pas toujours nécessaires à l'exercice du devoir d'information et de consultation. La question devra cependant être examinée de cas en cas.

Des employeurs souhaitent parfois procéder à une consultation plus individualisée, notamment en exposant clairement aux employés les conditions individuelles modifiées qu'il est envisagé de leur proposer à l'issue du transfert. Ils ont souvent le souci qu'à la fin de la procédure de la consultation, les employés soient en mesure d'accepter ou de s'opposer au transfert en pleine connaissance de cause d'une part. D'autre part, ils aimeraient que les employés puissent également, s'ils le souhaitent, accepter déjà à l'issue de la consultation que les nouvelles conditions (individualisées) s'appliquent dès la date du transfert. L'intérêt des employeurs est notamment d'harmoniser aussitôt que possible les conditions de travail au sein de leur personnel lorsque, suite au transfert une nouvelle population d'employés rejoint, chez l'acquéreur, une population déjà existante.

Une telle consultation « invidualisée » nécessitera ainsi un traitement de données nominatives en amont. La question de la pertinence de la base légale de l'art. 333a CO à titre de motif justificatif se pose en cas de consultation invidualisée. En effet, d'une part, cette norme n'impose pas de consultation individualisée. D'autre part cependant, elle n'est que relativement impérative et il n'est pas rare, par exemple, que des CCT prévoient des obligations d'information et de consultation plus étendues[46].

2. Le consentement de l'employé

Il convient d'abord de relever que l'article 328b CO est une disposition de droit semi-impératif. Il ne peut donc pas y être dérogé conventionnellement en défaveur du travailleur[47].

---

45 WYLER/HEINZER, p. 464 ; WILDHABER, pp. 376-377.

46 STREIFF/VON KAENEL/RUDOLPH, N 13 *ad* art 333a CO.

47 Art. 362 CO.

Nous avons retenu que l'article 328b CO énumère les buts qui peuvent légitimement être poursuivis par un employeur lorsqu'il traite des données de ses employés. Le traitement de données qui poursuit l'un de ces buts est présumé licite alors que tout traitement qui poursuit un autre but est présumé illicite.

Nous comprenons la nature semi-impérative de l'article 328b CO comme interdisant tout accord entre l'employé et l'employeur qui étendrait la présomption de licéité à d'autres buts que ceux énoncés par cette disposition. L'employé ne pourrait ainsi pas valablement accepter contractuellement que le traitement de ses données personnelles par son employeur dans un but étranger à l'examen de son aptitude à remplir son emploi ou à l'exécution du contrat de travail soit présumé licite.

En revanche, un traitement de données en principe illicite car ne bénéficiant pas de la présomption de l'article 328b CO peut-il être justifié dans un cas concret par le consentement de l'employé ? En d'autres mots, peut-on tenir compte du consentement de l'employé au vu du caractère semi-impératif de la disposition?

L'article 341 CO interdit à un employé de renoncer, pendant la durée du contrat et durant le mois qui suit la fin de celui-ci, aux créances résultant de dispositions impératives de la loi. Seule est interdite une renonciation unilatérale du travailleur à l'égard de l'employeur, mais non pas lorsque les parties parviennent à un arrangement impliquant des concessions réciproques. En d'autres termes, un employé peut valablement renoncer à une créance résultant d'une disposition impérative de la loi lorsqu'il a un intérêt propre suffisant pour justifier sa renonciation. L'exemple typique est celui d'une convention sur les modalités de fin des relations de travail par laquelle l'employé renonce à toute créance, existante et potentielle, contre son employeur et l'employeur lui verse une indemnité surobligatoire d'un montant adéquat.

La majorité des auteurs tire de l'article 341 CO la conclusion que le consentement de l'employé est un motif justificatif valable lorsque l'employé a un intérêt personnel au traitement de données envisagé[48]. L'exemple couramment cité par la doctrine est celui de l'employé qui consent à ce que son employeur fournisse des données concernant ses revenus au propriétaire d'un bien immobilier qu'il souhaite louer. L'examen de la solvabilité d'un candidat locataire est en effet exigé par les bailleurs et l'employé a un intérêt propre à ce que son employeur fournisse les informations utiles s'il veut obtenir le logement qu'il convoite.

[48] DUNAND, N 32 *ad* art. 328b CO ; STREIFF/VON KAENEL/RUDOLPH, N 3 *ad* art 328b CO ; BAUMANN, p. 639 ; MEIER, Due diligence, p.197 ; PÄRLI, N 8 et N 20 *ad* art. 328b CO.

Certains auteurs font un pas de plus et admettent que le consentement de l'employé à un traitement de ses données personnelles est un motif justificatif valable dès qu'il remplit les conditions posées par la LPD[49].

Selon l'article 4 alinéa 5 LPD, lorsque son consentement est requis pour justifier le traitement de données personnelles la concernant, la personne concernée ne consent valablement que si elle exprime sa volonté librement et après avoir été dûment informée. Pour être un motif justificatif valable au sens de la LPD, le consentement doit donc exprimer la libre volonté de l'employé après qu'il a été dûment informé[50]. En d'autres termes, le consentement doit être libre et éclairé[51]. Si le traitement concerne des données sensibles, le consentement doit au surplus être explicite.

Pour ces auteurs, le consentement de l'employé constitue un motif justificatif valable à un traitement de données hors du cadre de l'article 328b CO s'il est donné conformément aux principes de l'article 4 alinéa 5 LPD. La condition d'un intérêt propre de l'employé au traitement de ses données personnelles n'est pas nécessaire. Cette position se justifie si l'on considère que l'article 328b CO représente la concrétisation des principes de finalité et de proportionnalité dont le respect est imposé par la LPD. Ces principes sont violés si le traitement est effectué hors du cadre de l'article 328b CO.

La « créance » de l'employé découlant de l'article 328b CO consiste à notre sens dans le droit de l'employé à ce qu'un traitement de données hors du champ de l'aptitude ou de l'exécution du travail soit considéré de prime abord illicite sous l'angle notamment de l'article 12 alinéa 2 lettre a LPD et ne soit considéré admissible qu'en présence de motifs justificatifs.

En d'autres mots, l'employé ne peut pas contractuellement autoriser l'employeur à traiter toutes sortes de données personnelles hors du champ de l'art. 328b CO, en le dispensant de recourir à l'un ou l'autre des motifs justificatifs prévus par la LDP pour ce faire. Il ne peut pas renoncer à la présomption d'illicéité, qui ne peut être levée qu'en présence des motifs justificatifs.

À l'inverse, à notre sens, le caractère semi-impératif de la norme ne limite en rien l'admissibilité de l'ensemble des motifs justificatifs prévus par la LPD, notamment le consentement de la personne dont les données sont traitées.

Le consentement de l'employé à un traitement de données présumé de prime abord illicite n'est ainsi pas une dérogation à l'article 328b CO, mais bien un motif justificatif au sens

---

49 MEIER, Protection des données, N 857, p 328 et N 2040, pp. 652-653 ; BALZAN, p. 7.

50 Art. 4 al. 5 LPD.

51 MEIER, Protection des données, N 831 ss, pp. 318 ss ; MAURER-LAMBROU/STEINER, N 16f *ad* art. 4 LPD ; BAERISWYL, N 59-68 *ad* art. 4 LPD.

de l'article 13 de la LPD à laquelle l'art. 328b CO renvoie expressément. À ce stade, il suffit que le consentement de l'employé respecte les conditions de l'article 4 alinéa 5 LPD. En résumé, à notre sens, le caractère semi-impératif de l'art. 328b CO ne limite pas l'employé dans sa possibilité de délivrer, par son consentement, un motif justificatif au traitement de données qui ne seraient pas directement liées à son aptitude ou à l'exécution du contrat de travail.

L'employeur doit fournir aux employés dont le consentement est requis les informations utiles pour leur permettre de prendre une décision en toute connaissance de cause. L'étendue de l'information à donner doit être appréciée de cas en cas, en fonction notamment de la situation personnelle de l'employé et des circonstances concrètes de la transmission envisagée et du risque d'atteinte à la personnalité[52]. Suivant les cas, l'étendue de l'information nécessaire pour être complète au sens de la LPD pourrait exiger de fournir aux employés des éléments que les entités intéressées au projet de transaction considèrent confidentiels, à tout le moins au stade auquel le projet se trouve à ce moment. Il peut donc y avoir des tensions entre impératifs de confidentialité et volonté d'obtenir un consentement éclairé.

La personne concernée doit décider librement de donner son consentement ou non. Le simple fait qu'un refus puisse entraîner des conséquences négatives ne signifie pas en soi que le consentement n'est pas donné librement. En revanche, toute menace ou pression déraisonnable, directe ou indirecte, sur la personne concernée entraînerait l'invalidité du consentement. La situation de la personne concernée envers l'auteur du traitement doit être prise en compte dans l'examen de la liberté du consentement. Tel est le cas de la relation employeur – employé[53].

L'employeur qui veut obtenir le consentement libre et éclairé d'employés à la transmission de leurs données à l'acquéreur potentiel devrait ainsi préparer soigneusement la communication avec les employés concernés. Le traitement envisagé devrait leur être exposé, notamment ses motifs, sa finalité, son étendue et ses destinataires. L'employeur pourra mettre en avant les mesures de protection prévues (engagement de confidentialité imposé à l'acquéreur, traitement de données ayant lieu exclusivement en Suisse, etc.). Par mesure de précaution, l'employeur pourrait également préciser qu'un éventuel refus n'entraînerait aucune sanction de l'employé. L'employeur pourrait simultanément présenter les raisons pour lesquelles il souhaite que l'employé donne son consentement, notamment l'intérêt des données pour la conclusion de la transaction envisagée, voire les conséquences pratiques qui résulteraient si les données en cause n'étaient pas transmises.

---

52 MEIER, Protection des données, N 860-865, pp. 329-330 ; BAERISWYL, N 59 *ad* art. 4 LPD.

53 MEIER, Protection des données, N 851-858, pp. 326-328 ; BAERISWYL, N 65-68 *ad art.* 4 LPD.

Enfin, les employés doivent disposer d'un temps de réflexion adéquat avant de décider de donner leur consentement ou de le refuser. Exiger de leur part une réponse immédiate ou quasi-immédiate risquerait d'être considéré comme une pression déraisonnable. Il peut y avoir conflit avec les impératifs de calendrier du projet.

Le consentement sera plus aisé à obtenir s'il concerne des employés déjà impliqués dans la planification de la transaction (membres de la direction, RHs, cadres susceptibles d'entrer en contact personnellement avec l'acquéreur potentiel au cours du projet) et travaillant au bon succès du projet.

Il pourra être également aisé à obtenir des personnes dont la transmission est requise aux fins de leur proposer des conditions avantageuses, par exemple lorsque l'acquéreur potentiel souhaite d'ores et déjà soumettre des offres écrites de rétention à des *key employees*, sous la condition suspensive de la bonne réalisation de la transaction.

3. Un intérêt prépondérant privé ou public

L'article 13 alinéa 2 LPD énumère, à titre exemplaire, des cas dans lesquels les intérêts prépondérants de la personne qui traite des données personnelles entrent en considération. Selon sa lettre a, tel est le cas lorsque le traitement est en relation directe avec la conclusion d'un contrat et que les données traitées concernent le cocontractant de l'auteur du traitement.

Les auteurs sont divisés sur la question de savoir si, dans le cadre d'un projet de fusion ou de transfert d'entreprise, cette disposition permet le traitement de données personnelles des employés du cocontractant. Pour certains, seules les données du cocontractant lui-même peuvent être traitées sous couvert de l'article 13 alinéa 2 lettre a LPD. L'acquéreur potentiel peut ainsi se prévaloir de l'article 13 alinéa 2 lettre a LPD pour justifier qu'il traite des données concernant l'entreprise-cible. En revanche cette disposition ne lui est d'aucun secours pour justifier le traitement de données des employés de celle-ci dès lors que les employés ne sont pas des cocontractants dans la transaction envisagée[54]. Pour d'autres auteurs, l'article 13 alinéa 2 lettre a LPD doit être étendu aux données concernant les employés du cocontractant lorsque le traitement a lieu dans le cadre d'une vérification préalable (*due diligence*)[55].

À notre avis, il peut faire sens de considérer que les données relatives aux employés d'une entreprise entrent dans le champ des données de cette entreprise (cocontractant) dans le cadre de l'article 13 alinéa 2 lettre a LPD. Les employés sont bien une composante

---

54 WERMELINGER, N 19 *ad* art. 13 LPD ; RAMPINI N 32 *ad* art. 13 LPD.

55 MEIER, Protection des données, N 1662, p. 548 et N 1609 ; PFPDT, Transmission de données, p. 2 qui précise toutefois, sans autre justification, que les informations ne peuvent pas être transmises à un acheteur potentiel avec référence nominale.

importante de l'entreprise elle-même, et donc du cocontractant. Les données des employées, dans la mesure où elles sont liées aux rapports de travail, sont également des données concernant leur employeur (le contractant). L'acquéreur potentiel pourrait ainsi faire valoir son intérêt prépondérant au sens de cet article pour justifier sa prise de connaissance de données sur les employés de l'entreprise-cible.

En revanche, cette disposition n'est pas, directement à tout le moins, invocable par l'employeur qui entend transmettre des données personnelles de ses employés à son cocontractant potentiel. On rappelle en effet que l'article 13 alinéa 2 lettre a LPD admet de prendre en considération les intérêts prépondérants de la personne qui traite des données personnelles si les données traitées concernent le cocontractant. Ici, la personne qui traite des données est l'employeur, soit l'entreprise-cible. Les données transmises concernent ses propres employés; elles ne concernent en rien le cocontractant, soit l'acquéreur potentiel.

Cette liste de l'article 13 al. 2 LPD n'est cependant pas exhaustive. La possibilité que la transmission de données personnelles des employés soit justifiée par un intérêt prépondérant de l'employeur dépendra d'une balance des intérêts qui devra tenir compte de toutes les circonstances de l'espèce.

L'intérêt de l'employeur à transmettre les informations requises par l'acquéreur, et celui-ci à les traiter devra être mis en balance avec le risque d'atteinte à la personnalité des employés concernés. Il s'agit donc d'une question d'appréciation. Le résultat de la pesée d'intérêts peut évoluer au fil des enjeux et préoccupations rencontrés durant le déroulement du processus jusqu'à l'accomplissement du transfert.

L'intérêt au traitement de données peut être plutôt financier dans les premiers temps du projet (pouvoir évaluer le coût du projet, le coût de la masse salariale, la situation des *key employees*, le coût d'éventuels licenciements). Il pourra ensuite être plus tourné sur des préoccupations légales et pratiques, en plus qu'économiques (quelles modifications envisager pour les employés, quelles informations traiter pour accomplir les procédures d'information et de consultation, etc.) puis enfin, toutes aussi légales et pratiques, des préoccupations liées au bon respect des obligations du contrat de travail (comment être prêt, au jour du transfert, à respecter toutes ses obligations d'employeur.

Du côté de l'employé, plus le transfert devient certain et proche, moins il aura d'intérêt à s'opposer à ce que son futur employeur puisse déjà traiter des données le concernant, si ce n'est à retarder de quelques jours à quelques semaines, la prise de connaissance par ce futur employeur de données qu'il sera dans tous les cas en droit de connaître et traiter lorsqu'il aura cette qualité.

V. Transmission des données des employés après le transfert de l'entreprise

En vertu de l'article 333 CO les rapports de travail passent à l'acquéreur avec tous les droits et les obligations qui en découlent, au jour du transfert, à moins que le travailleur ne s'y oppose.

En cas d'opposition d'un employé, les rapports de travail prennent fin à l'expiration du délai de congé légal mais au plus tôt au jour du transfert. Si le délai de congé légal n'est pas échu au jour du transfert, les rapports de travail passent à la nouvelle entité au moment du transfert, pour prendre ensuite définitivement fin à l'expiration du délai de congé légal[56].

Dès l'entrée en vigueur du contrat de fusion ou de transfert d'entreprise, l'acquéreur devient ainsi de par la loi l'employeur de tous les employés de l'entreprise-cible, sous la seule réserve des employés dont le contrat de travail a pris fin le même jour en raison de leur opposition.

En sa qualité d'employeur, l'acquéreur peut se prévaloir de l'article 328b CO. Il est autorisé par cette disposition légale à traiter les données personnelles de ses (nouveaux) employés qui portent sur les aptitudes du travailleur à remplir son emploi ou sont nécessaires à l'exécution du contrat de travail.

L'entreprise-cible, dans la mesure où elle perd la qualité d'employeur, peut-elle se prévaloir d'une disposition légale qui justifie qu'elle remette au nouvel employeur les données personnelles de ses ex-employés ?

Il est généralement admis que le dossier contenant les données personnelles des employés fait partie des rapports de travail et que leur transfert à l'acquéreur est couvert par l'article 333 CO[57]. L'étendue des données qui sont transmises au jour du transfert est toutefois limitée par l'article 328b CO. Ainsi, toutes les données nécessaires à l'acquéreur pour assumer ses obligations d'employeur dans la continuité du rapport de travail doivent passer à l'acquéreur. Il faut garder à l'esprit que le nouvel employeur sera responsable notamment de rédiger les certificats de travail au départ de chaque employé et que ces certificats devront porter sur la durée totale de la relation de travail, y compris la période d'emploi au sein de l'entreprise-cible. Les données nécessaires à la rédaction de ces certificats doivent donc lui être transmises. En revanche, des données anciennes qui ne sont plus

---

56 WYLER/HEINZER, pp. 462-463 ; STREIFF/VON KAENEL/RUDOLPH, N 12 *ad* art. 333 CO ; CHENAUX/MARTIN, N 20 *ad* art. 333 CO.

57 MAURER-LAMBROU/STEINER, N 21 *ad* art. 4 LPD ; BAUMANN, p. 646 ; GERICKE/BURRI, N 24.65, p. 894.

pertinentes pour l'exécution du contrat de travail et des obligations liées ne peuvent être considérées comme incluses dans le rapport de travail.

Compte tenu des délais de prescription des créances en droit du travail, qui sont de cinq ou dix ans suivant les prétentions, le nouvel employeur doit néanmoins recevoir toutes les données en lien avec la relation de travail qui peuvent être pertinentes pour juger de prétentions non prescrites. Si de telles données figurent encore dans le dossier d'un employé tenu par l'entreprise-cible, elles doivent être détruites avant le transfert du dossier à l'acquéreur.

VI. Conclusion

Tout transfert d'entreprise, quelle que soit sa forme juridique, implique nécessairement que des données personnelles des employés soient transmises à l'acquéreur. La reprise des rapports de travail par l'acquéreur, que la loi impose, exige que toutes les données nécessaires à la poursuite du contrat de travail lui soient communiquées. L'obligation légale d'informer les employés avant le transfert des conséquences que celui-ci aura sur leur situation implique que leurs conditions de travail en vigueur soient transmises à l'acquéreur afin que ces conséquences puissent être définies. Enfin, avant de s'engager dans une transaction par la signature d'un contrat de fusion ou de transfert d'entreprise, l'acquéreur a besoin d'évaluer la situation globale de l'entreprise-cible, dont les employés sont un élément essentiel. L'employeur doit néanmoins s'assurer que ce traitement nécessaire des données personnelles de ses employés soit exécuté dans le respect des dispositions légales sur la protection des données. Il lui revient, dans chaque étape de la transaction et suivant toutes les circonstances du projet en cause, de déterminer quelles données il est en droit de communiquer et sous quelle forme. Il s'agit d'une analyse individuelle à chaque transaction, qui évolue au cours de celle-ci. Elle ne peut se réduire à un modèle prédéfini applicable de façon standardisée.

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.

BAERISWYL BRUNO, Commentaire de l'art. 4 LPD, *in* : Bruno Baeriswyl/Kurt Pärli (éds.), Datenschutzgesetz (DSG) – Handkommentar, Berne 2015.

BALZAN MARIE-CHRISTINE, La protection des données personnelles des travailleurs dans la due diligence, *in* : Rémy Wyler (éd.), Panorama II en droit du travail, Berne 2012, pp. 3-20.

BAUMANN ROBERT, Die Übertragung von Arbeitnehmerdaten bei Betriebsübergängen, *in* : PJA 2004, pp. 638-648.

BLECHTA GABOR-PAUL, Commentaire de l'art 3. LPD, *in* : Urs Maurer-Lambrou/Gabor-Paul Blechta (éds.), Datenschutzgesetz/Öffentlichkeitsgesetz – Basler Kommentar, 3e édition, Bâle 2014.

CHENAUX JEAN-LUC/MARTIN FRANÇOISE, Commentaire des art. 333 et 333a CO, *in* : Jean-Philippe Dunand/Pascal Mahon (éds.), Commentaire du contrat du travail, Berne 2013.

CONSEIL FÉDÉRAL, Message concernant la loi fédérale sur la protection des données (LPD) du 23 mars 1988, FF 1988 II 421, (cité : Message LPD).

DUNAND JEAN-PHILIPPE, Commentaire de l'art. 328b CO, *in* : Jean-Philippe Dunand/Pascal Mahon (éds.), Commentaire du droit du travail, Berne 2013, pp. 317-355.

FEY MARCO, Commentaire de l'art. 1 LPD, *in* : Bruno Baeriswyl/Kurt Pärli (éds.), Datenschutzgesetz (DSG) – Handkommentar, Berne 2015.

GERICKE DIETER, M&A und Datenschutz, *in* : RSJ 99/2003, pp. 1-13.

GERICKE DIETER/BURRI CHRISTOF, Datenschutz bei Veräusserung und Zusammenschluss von Unternehmen, *in* : Nicolas Passadelis/David Rosenthal/Hanspeter Thür (éds.), Datenschutzrecht : Beraten in Privatwirtschaft und öffentlicher Verwaltung, Bâle 2015, pp. 869 ss.

MAURER-LAMBROU URS/KUNZ SIMON, Commentaire des art. 1 et 12 LPD, *in* : Urs Maurer-Lambrou/Gabor-Paul Blechta (éds.), Datenschutzgesetz/Öffentlichkeitsgesetz – Basler Kommentar, 3e édition, Bâle 2014.

MAURER-LAMBROU URS/STEINER ANDREA, Commentaire de l'art. 4 LPD, *in* : Urs Maurer-Lambrou/Gabor-Paul Blechta (éds.), Datenschutzgesetz/Öffentlichkeitsgesetz – Basler Kommentar, 3e édition, Bâle 2014.

MEIER ERIC OLIVIER, Due diligence bei Unternehmensübernahmen, Zurich 2010 (cité : MEIER, Due diligence).

MEIER PHILIPPE, Protection des données, Fondements, principes généraux et droit privé, Berne 2010 (cité : MEIER, Protection des données).

MEYER MIRJAM, Rechtsrisiken und Rechtsrisikomanagement bei M&A-Transaktionen unter besonderer Berücksichtigung des schweizerischen Rechts, Zürcher Studien zum Privatrecht 256, Zurich 2013.

PÄRLI KURT, Commentaire de l'art. 328b CO, *in* : Bruno Baeriswyl/Kurt Pärli (éds.), Datenschutzgesetz (DSG) – Handkommentar, Berne 2015.

PRÉPOSÉ FÉDÉRAL À LA PROTECTION DES DONNÉES ET À LA TRANSPARENCE, Transmission de données lors de concentrations d'entreprises, état mars 2010 (cité : PFPDT, Transmission de données).

RAMPINI CORRADO, Commentaire des art. 12 et 13 LPD, *in* : Urs Maurer-Lambrou/Gabor-Paul Blechta (éds.), Datenschutzgesetz/Öffentlichkeitsgesetz – Basler Kommentar, 3e édition, Bâle 2014.

REHBINDER MANFRED/STÖCKLI JEAN-FRITZ, Der Arbeitsvertrag – Berner Kommentar, 2e édition, Berne 2014.

RUDIN BEAT, Commentaire de l'art. 3 LPD, *in* : Bruno Baeriswyl/Kurt Pärli (éds.), Datenschutzgesetz (DSG) – Handkommentar, Berne 2015.

STREIFF ULLIN/VON KAENEL ADRIAN/RUDOLPH ROGER, Arbeitsvertrag – Praxiskommentar zu Art. 319-362 OR, 7e édition, Zurich/Bâle/Genève 2012.

WERMELINGER AMÉDÉO, Commentaire des art. 12 et 13 LPD, *in* : Bruno Baeriswyl/Kurt Pärli (éds.), Datenschutzgesetz (DSG) – Handkommentar, Berne 2015.

WILDHABER ISABELLE, Das Arbeitsrecht bei Umstrukturierungen, Zurich 2011.

WYLER RÉMY/HEINZER BORIS, Droit du travail, 3e édition, Berne 2014.

VALÉRIE DÉFAGO GAUDIN, JEAN-PHILIPPE DUNAND et AUDREY VOUTAT

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

Sommaire

		Page
I.	Introduction	143
II.	Le salaire, la rétribution	145
	A. En droit privé du travail	145
	B. En droit de la fonction publique	145
III.	À quelles conditions, l'employeur peut-il communiquer le salaire à des tiers ?	147
	A. En droit privé du travail	147
	1. La communication du salaire à un tiers constitue une atteinte potentielle à la personnalité du travailleur	147
	a) Protection de la personnalité (art. 328 CO)	148
	b) Protection des données (art. 328b CO et LPD)	149
	2. Motifs justificatifs	152
	a) Système général	152
	b) Base légale	153
	aa) Données nécessaires à l'exécution du contrat de travail	153
	bb) Externalisation	154
	cc) Calcul de la participation aux bénéfices	155
	dd) Sociétés cotées en bourse	155
	c) Intérêt prépondérant privé ou public	157
	aa) Participation aux bénéfices	158
	bb) Bonus	158
	cc) Egalité salariale selon la LEg	159
	d) Consentement	161
	3. Respect des principes généraux	162
	a) Limitation de l'accès aux données salariales	162
	b) Protection des données salariales contre le vol	163
	c) Communication des données salariales à une société commerciale	163
	4. Réserve en faveur des lois sur la transparence	164
	B. En droit de la fonction publique	164
	1. Protection de la personnalité de l'agent public	164
	2. Protection des données et transparence	167
	a) Fonction publique fédérale (art. 27ss LPers, LPD et LTrans)	167
	aa) Champ d'application de la LPD	167

bb) Exigence d'une base légale. Extension de la notion de données sensibles ? 168
cc) La communication de données personnelles 169
dd) Le principe de transparence 169
ee) Le salaire des employés de la Confédération 171
ff) Les activités accessoires des employés de la Confédération 172
b) Fonction publique cantonale (CPDT-JUNE) 173

IV. À quelles conditions un travailleur peut-il communiquer son salaire à un tiers ? 174
A. En droit privé du travail 175
1. Intérêts en présence 175
a) Liberté de l'employé 175
b) Protection de l'employeur 176
c) Devoir de diligence et de fidélité 176
d) Protection des secrets d'affaires 176
2. Pesée des intérêts 178
a) Communication du salaire à des collègues de travail 178
b) Critique de la politique salariale de l'entreprise 179
c) Communication du salaire à un concurrent 180
3. Clause de confidentialité 180
B. En droit de la fonction publique 182
1. Le devoir de fidélité 182
2. La communication du salaire à des tiers 183
3. La critique de la politique salariale de l'État 184

V. Quelle est la valeur d'une clause de confidentialité contenue dans une convention de départ ? 185
A. En droit privé du travail 186
1. Accord de résiliation 186
a) Accord librement consenti 186
b) Accord contenant des concessions réciproques 186
c) Accord invalide 187
2. Clause de confidentialité 187
B. En droit de la fonction publique 188
1. Les conventions de départ en droit de la fonction publique 188
2. Le principe de transparence 189

VI. Conclusion 189

Bibliographie 192

I. Introduction

Selon la définition du *Petit Robert*, sont confidentielles les informations qui doivent rester secrètes ou qui ne s'adressent qu'à un petit nombre de personnes[1]. Nous chercherons à déterminer dans notre contribution dans quelle mesure le salaire constitue une information confidentielle.

Comptant parmi les quatre éléments caractéristiques du contrat de travail, le salaire constitue la prestation principale que l'employeur fournit au travailleur en contrepartie du travail fourni (cf. art. 319 al. 1 CO)[2]. En droit de la fonction publique, les notions de traitement ou de rétribution sont utilisées dans les statuts traditionnels pour désigner la contreprestation du travail fourni par l'agent public ; désormais, la notion de salaire apparaît dans les statuts modernisés, comme dans la Loi sur le personnel de la Confédération du 24 mars 2000[3].

La présente contribution est consacrée au caractère confidentiel du salaire, respectivement de la rétribution de l'agent public. Il s'agit plus particulièrement de déterminer dans quelle mesure le montant du salaire d'un travailleur peut être communiqué, par l'employeur ou le travailleur lui-même, à des tiers. Comme le relève le Préposé fédéral à la protection des données et à la transparence, il est difficile en la matière « d'appliquer des formules à l'emporte-pièce », car deux intérêts contradictoires qui caractérisent notre société s'opposent : la transparence et la protection de la personnalité[4].

Suivant les cas, le travailleur préfèrera la confidentialité ou la transparence ; il en va de même de l'employeur. S'agissant du travailleur, on postule généralement que la protection de sa personnalité impose une certaine confidentialité du salaire. Dans le même temps cependant, des auteurs ont souligné que « dans leur préoccupation légitime d'améliorer leurs conditions salariales », les travailleurs « ont un intérêt réel à connaître la rémunération de leurs collègues » ; le droit de tout travailleur « de rendre public le montant exact de sa rémunération » fait ainsi partie des droits de sa personnalité[5]. On voit donc qu'il conviendra de traiter la question de manière nuancée.

---

1 Le Petit Robert – Dictionnaire alphabétique et analogique de la langue française, Paris 2016, p. 505.

2 DUNAND, N 23 *ad* art. 319 CO, p. 7.

3 LPers, RS 172.220.1. Pour faciliter la distinction entre le régime de droit privé et de la fonction publique, nous nous référerons le plus souvent à la notion de traitement dans celui-ci.

4 Cf. la notice du Préposé fédéral à la protection des données et à la transparence sur la sphère privée des employés, p. 2, consultable sur le site du préposé à l'adresse : www.edoeb.admin.ch > Secteur du travail > Sphère privée (site consulté le 8 janvier 2017).

5 BRUNNER/BÜHLER/WAEBER/BRUCHEZ, N 12 *ad* art. 328 CO, p. 147.

À cette pondération s'ajoute, s'agissant de la rétribution des agents de la fonction publique, le fait que les rémunérations sont prévues par la loi, donc par définition accessibles à tous, et que l'obligation de transparence est imposée par les lois *ad hoc*. La difficulté de l'analyse réside alors non seulement dans la pondération matérielle des divers intérêts opposés, mais également, et avant tout, dans la détermination des champs d'application des trois corps de règles régissant le statut des agents, la protection des données et la transparence, qui ne se recoupent pas nécessairement. En outre, la législation en matière de transparence est dans certaines circonstances susceptible de s'appliquer également à des entités privées pour leurs rapports de droit privé du travail avec leurs employés.

Le thème de la confidentialité du salaire relève autant du droit que d'autres disciplines comme l'économie, la psychologie, la sociologie ou l'anthropologie. Nous nous concentrerons ici sur les aspects juridiques. Notre objectif sera de répondre aux trois questions suivantes, après avoir défini les contours des notions de salaire et de rétribution (**chapitre II**) :

- L'employeur peut-il communiquer le salaire à des tiers (**chapitre III**) ?
- Le travailleur peut-il communiquer son salaire à des tiers (**chapitre IV**) ?
- Une convention de départ peut-elle comporter une clause de confidentialité qui interdit toute communication du salaire à des tiers (**chapitre V**) ?

Les questions soulevées sont pertinentes autant en droit privé du travail que dans le droit de la fonction publique. Notre contribution aura donc un aspect pluridisciplinaire qui permettra de souligner les convergences et les divergences entre ces deux régimes. Pour ce qui est du droit de la fonction publique, nous nous référerons au droit du personnel de la Confédération, qui a opté pour la voie contractuelle pour la relation avec ses agents, ainsi qu'au droit cantonal neuchâtelois, qui consacre un statut dit traditionnel de la fonction publique. Nous ne traiterons en revanche pas des conséquences d'une communication illicite par l'employeur ou le travailleur puisque les sanctions et procédures sont présentées dans un article détaillé du présent ouvrage[6]. Enfin, nous ne tiendrons pas compte de l'avant-projet de révision totale de la loi sur la protection des données qui fait également l'objet d'une contribution volumineuse dans l'ouvrage[7].

6 Cf. la contribution de WITZIG, pp. 25 ss.
7 Cf. la contribution de DUBOIS, pp. 47 ss.

II. Le salaire, la rétribution

A. En droit privé du travail

Au sens large, le salaire désigne l'ensemble des contre-prestations que doit l'employeur en échange des prestations de services du travailleur. Il comprend le salaire fixe, ainsi que de nombreuses autres formes de rémunération qui peuvent être dues dans un cas d'espèce, tels que le 13e salaire, le salaire en nature (cf. par exemple art. 322 al. 2 CO), la participation au résultat de l'exploitation (art. 322a CO), la provision (art. 322b CO), la gratification (art. 322d CO) ou autre bonus, le salaire à la pièce ou à la tâche (art. 326 CO) et le salaire afférent aux vacances (art. 329d al. 1 CO). Il comprend également divers suppléments spécifiques, comme la rémunération des heures supplémentaires (art. 321c CO), du travail supplémentaire (art. 13 LTr), du travail de nuit (art. 17b LTr) ou du travail le dimanche (art. 19 LTr), de même que certaines indemnités, telles que l'indemnité à raison de longs rapports de travail (art. 339b CO) ou les indemnités de départ.

En droit suisse, le salaire dû au travailleur est régi, en règle générale, par le principe de la liberté contractuelle[8]. En effet, l'art. 322 al. 1 CO prévoit que l'employeur paie au travailleur le salaire convenu. Les parties fixent donc librement le montant du salaire. Le principe de la liberté contractuelle rencontre toutefois de nombreuses limites qui résultent soit de l'art. 322 al. 1 CO, soit d'autres dispositions légales[9]. En effet, les conventions collectives de travail (art. 356 ss CO), les contrats types de travail (art. 359 ss CO), l'interdiction de discriminer les travailleurs à raison du sexe (art. 8 al. 3 Cst. et art. 3 LEg), ou encore les règles applicables en matière de location de services (art. 20 LSE), de détachement de travailleurs (art. 2 LDét) et de police des étrangers (art. 22 LEtr) peuvent imposer des salaires déterminés dans leurs champs d'application respectifs. Enfin, l'art. 322 al. 1 CO précise qu'à défaut de salaire convenu ou fixé par un contrat type de travail ou par une convention collective de travail, l'employeur doit payer au travailleur le salaire « usuel ».

B. En droit de la fonction publique

En droit de la fonction publique, la relation entre la collectivité publique et son agent est régie par le principe de la légalité (art. 5 al. 1 de la Constitution fédérale de la

8 CARRUZZO, N 4 *ad* art. 322 CO, p. 112 ; DANTHE, N 12 *ad* art. 322 CO, p. 139.

9 Sur les restrictions de la liberté contractuelle en matière de fixation du salaire, cf. CARRUZZO, pp. 113 ss ; DANTHE, pp. 139 s.

Confédération suisse du 18 avril 1999[10]). La rétribution versée à l'agent public en contrepartie de son travail n'est donc pas fixée librement, mais découle de la loi.

Pour le personnel fédéral, le salaire dépend de la fonction, de l'expérience et de la prestation (art. 15 al. 1 LPers). Lors de l'engagement, l'employé est affecté à une classe de salaire de 1 à 38 en fonction de sa formation, de son expérience professionnelle et extra-professionnelle, ainsi que du marché de l'emploi (art. 36 et 37 al. 1 de l'Ordonnance sur le personnel de la Confédération du 3 juillet 2001[11]). Le salaire évolue ensuite en fonction de l'évaluation personnelle de l'employé sur la base des objectifs convenus en matière de prestations, de comportement et de compétences (art. 15 al. 3 OPers). Selon l'échelon d'évaluation, qui va de 1 (insuffisant) à 4 (très bien) (art. 17 OPers), l'augmentation varie de 0,5% à 3% jusqu'à ce que le montant maximal de la classe de salaire soit atteint ; une prestation insuffisante peut donner lieu à une réduction de salaire jusqu'à 2% (art. 39 OPers). Des suppléments au salaire peuvent être versés, comme notamment l'indemnité de résidence (art. 43 OPers), la compensation du renchérissement (art. 44 OPers), des indemnités pour le travail du dimanche et de nuit ou le service de permanence (art. 45 OPers), la prime de fonction en contrepartie de tâches exigeantes (art. 46 OPers), l'allocation spéciale pour compenser des risques ou des conditions pénibles de travail (art. 48 OPers), une prime de prestations pour des prestations supérieures à la moyenne et des engagements particuliers (art. 49 OPers) ou une allocation liée au marché de l'emploi pour attirer ou fidéliser un personnel aux compétences reconnues (art. 50 OPers). À noter également qu'il existe un salaire minimal (art. 15 al. 2 LPers et 7 de l'Ordonnance-cadre relative à la loi sur le personnel de la Confédération du 20 décembre 2000[12]).

Pour le personnel de l'administration cantonale neuchâteloise, le traitement est fixé lors de l'engagement de l'agent public en fonction de sa formation et de son expérience (art. 53 al. 2 de la Loi sur le statut de la fonction publique du 28 juin 1995[13]). Il évolue ensuite année après année, au rythme d'un échelon sur les 38 que compte chacune des 16 classes de traitement de la fonction publique (art. 6, 7 et 19 du Règlement concernant les traitements de la fonction publique du 9 mars 2005[14], étant précisé que les montants minimaux et maximaux des traitements figurent en annexe de la LSt). Le traitement des fonctionnaires comprend le traitement de base, l'allocation de renchérissement et diverses allocations éventuelles (art. 52 LSt), notamment une allocation complémentaire pour l'entretien d'enfants (art. 58 LSt), une prime de fidélité (art. 59 LSt), une rétribution

10 Cst., RS 101.

11 OPers, RS 172.220.111.3. Le salaire maximal est de CHF 60'764.- pour la classe 1 et de CHF 370'568.- pour la classe 38.

12 Ordonnance-cadre LPers, RS 172.220.11. Celui-ci est de CHF 38'000.-.

13 LSt, RSN 152.510.

14 RTFP, RSN 152.511.10.

spéciale pour services de nature exceptionnelle (art. 61 LSt), une indemnité pour remplacement (art. 38 RTFP), une indemnité pour travaux spéciaux (art. 38 RTFP), une prime de fidélité (art. 20 du Règlement général d'application de la loi sur le statut de la fonction publique du 9 mars 2005[15]) ou une indemnisation pour le service de piquet (art. 40a RTFP et Arrêté réglant les modalités de validation et de rémunération du service de piquet dans l'administration cantonale du 28 juin 2010[16]).

III. À quelles conditions, l'employeur peut-il communiquer le salaire à des tiers ?

Pour diverses raisons, l'employeur doit nécessairement traiter, conserver et diffuser le montant du salaire de ses employés à des tiers. Il s'agit ici de préciser à quelles conditions. Déterminer les textes applicables est très important pour aborder la question : la protection de la personnalité repose sur des sources différentes en droit privé et en droit de la fonction publique ; de plus, la législation fédérale en matière de protection des données s'applique à la relation de travail de droit privé et à la fonction publique fédérale, mais non à la fonction publique cantonale ; de plus la même législation sur la protection des données prévoit des règles différentes selon que l'entité qui traite les données est une entité privée ou une entité publique ; enfin, les règles sur la transparence, qui s'appliquent en principe à l'administration, peuvent aussi selon les cas s'appliquer aux employeurs privés.

A. En droit privé du travail

Le salaire d'un travailleur constitue un élément de sa personnalité dont la confidentialité est protégée par la loi (**1.**). L'employeur n'est en droit de collecter, de conserver ou de diffuser ce renseignement personnel que s'il peut se prévaloir d'un motif justificatif (**2.**) et, qu'en outre, le traitement respecte certains principes généraux du droit, tels que la bonne foi et la proportionnalité (**3.**).

1. La communication du salaire à un tiers constitue une atteinte potentielle à la personnalité du travailleur

La personnalité englobe l'ensemble des biens qui appartiennent à toute personne physique ou morale du seul fait de son existence[17]. Les articles 28 ss CC constituent une protection générale contre les atteintes à la personnalité provenant de tiers. Dans les relations de

[15] RSt, RSN 152.511.
[16] RSN 152.511.102.
[17] JEANDIN, N 14 *ad* art. 28 CC, p. 248.

travail soumises au code des obligations, ils sont complétés par des dispositions spécifiques qui visent à protéger la personnalité des travailleurs, soit en général (**a**), soit plus précisément dans le cadre du traitement des données les concernant (**b**).

a) Protection de la personnalité (art. 328 CO)

Selon l'art. 328 CO, l'employeur protège et respecte, dans les rapports de travail, la personnalité du travailleur. Lorsque l'employeur est une personne morale, il faut lui imputer les actes de ses organes (cf. art. 55 al. 2 CC)[18]. Par ailleurs, l'employeur répond également des actes de ses auxiliaires (cf. art. 55 et 101 CO)[19]. L'article 328 CO intègre et concrétise, dans le contrat de travail, les principes généraux de protection de la personnalité qui sont énoncés aux articles 27 ss CC[20]. L'article 328 CO constitue une norme semi-impérative, soit une disposition à laquelle il ne peut être dérogé, par accord, contrat type de travail ou convention collective de travail, au détriment du travailleur (cf. art. 362 CO).

La protection de la personnalité du travailleur constitue l'un des principes cardinaux du droit du travail dont l'importance ne cesse de croître[21]. Elle revêt une importance particulière dans les rapports de travail en raison du rapport de subordination du travailleur à l'égard de l'employeur[22]. Elle constitue d'ailleurs le pendant du devoir de fidélité du travailleur énoncé à l'article 321a CO[23]. Pour rappel, la personnalité du travailleur comprend « tous les biens personnels du travailleur qui sont inséparables de son être physique et moral et de sa qualité de membre de la société »[24]. Les valeurs protégées sont notamment l'intégrité physique, la santé physique et psychique, l'intégrité morale et la considération sociale, les libertés individuelles, ainsi que la sphère privée[25].

Dans le contexte de ce chapitre, le salaire nous paraît avoir plus particulièrement des liens avec la considération sociale et la sphère privée du travailleur. La considération sociale comprend l'honneur personnel et professionnel, la réputation économique, ainsi que la considération dans et à l'extérieur de l'entreprise[26]. Quant à la sphère privée, on peut en préciser la notion en tenant compte de la « théorie des sphères », selon laquelle il convient

---

18 ATF 128 III 76, c. 1b ; TF 4A_544/2008 du 10 février 2009, c. 2.3.

19 ATF 137 III 303, c. 2.2.2 ; ATF 125 III 70, c. 3a.

20 DUNAND, N 1 *ad* art. 328, p. 270.

21 Cf. DUNAND, Protection, pp. 47 ss.

22 TF 2C_103/2008 du 30 juin 2008, c. 6.2.

23 ATF 132 III 257, c. 5.1, *in* : JdT 2007 I 274, SJ 2007 I 173.

24 Message du Conseil fédéral à l'Assemblée fédérale concernant la révision des titres dixième et dixième bis du code des obligations du 25 août 1967, *in* : FF 1967 II 249 (353).

25 BRUNNER/BÜHLER/WAEBER/BRUCHEZ, N 2 *ad* art. 328 CO, p. 141.

26 ATF 131 III 535, c. 4.3.

de distinguer sphère intime ou secrète, sphère privée et sphère publique ou commune[27]. La sphère intime comprend les faits et gestes qui, de par leur nature, sont soustraits à la connaissance d'autrui, à l'exception des personnes auxquelles ils ont été destinés ou spécialement confiés[28]. La sphère privée se compose quant à elle, d'évènements ou d'informations qui ne concernent pas la vie intime, mais que chacun décide de ne partager qu'avec un nombre restreint de personnes auxquelles il est attaché par des liens relativement étroits[29]. Enfin, la sphère publique comprend tous les faits et gestes qui sont accessibles à la connaissance de tous et qui peuvent être divulgués sans autorisation[30]. Selon la jurisprudence et la doctrine, seules les sphères intime et privée, qui forment la vie privée, sont protégées par les droits de la personnalité[31].

Le montant du salaire d'un travailleur ne constitue pas un simple nombre dépourvu de toute composante personnelle, mais est, au contraire, un révélateur de nombreux aspects de sa personnalité. Il reflète notamment sa formation, son expérience professionnelle, ainsi que ses prédispositions (positives ou négatives) en matière de négociation (salariale). Le salaire du travailleur relève évidemment de la considération sociale de ce dernier. Selon les usages pratiqués dans notre pays, dans lequel règne une certaine discrétion en la matière, le salaire nous paraît également relever de sa sphère privée.

En conclusion, le salaire constitue un élément de la personnalité des employés dont la confidentialité est protégée par l'article 328 CO.

b) Protection des données (art. 328b CO et LPD)

La Loi sur la protection des données du 19 juin 1992[32] régit le traitement des données effectué par, notamment, des personnes privées (art. 2 al. 1 let. a LPD)[33].

La législation sur la protection des données ne protège évidemment pas les données, mais « la personnalité et les droits fondamentaux des personnes qui font l'objet d'un traitement de données » (cf. art. 1 LPD). Alors que la loi sur la protection des données concrétise la protection générale de la personnalité, le législateur a souhaité adopter une disposition spécifique pour régler la protection des données dans les relations de travail, à savoir l'article 328b CO. Il faut dire que l'employeur collecte et traite de nombreuses données

---

27 Cf. AUBERSON, pp. 173 ss.
28 JEANDIN, N 40 *ad* art. 28 CC, p. 254.
29 JEANDIN, N 41 *ad* art. 28 CC, pp. 254 s.
30 JEANDIN, N 42 *ad* art. 28 CC, p. 255.
31 ATF 118 IV 41, *in* ; JdT 1994 IV 79 ; AUBERSON, p. 173 ; JEANDIN, N 43 *ad* art. 28 CC, p. 255.
32 LPD, RS 235.1.
33 Elle s'applique également aux organes fédéraux, voir *infra*, pp. 167 ss.

personnelles de ses employés, de toute nature et pendant une longue durée[34]. Les employés sont donc exposés à des atteintes importantes à leur personnalité.

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. En outre, les dispositions de la loi fédérale du 19 juin 1992 sur la protection des données sont applicables ». L'art. 328b CO complète et précise la protection de la personnalité des travailleurs prévue à l'art. 328 CO en désignant le type de données personnelles que l'employeur peut traiter et en renvoyant à la LPD. Tout comme l'article 328 CO, l'article 328b CO est une norme semi-impérative (cf. art. 362 CO).

La LPD définit autant la notion de « donnée » que celle de « traitement ». Sont considérées comme données personnelles toutes les informations qui se rapportent à une personne identifiée ou identifiable (art. 3 let. a LPD). Il s'agit, dans les relations de travail, de tous renseignements, indications ou notes concernant la personne du travailleur, et qui portent tant sur sa vie privée que sur sa vie professionnelle, que le support soit manuel ou informatique, et que les données aient été recueillies par l'employeur lui-même ou par un tiers auquel il a confié cette tâche[35].

Pour que l'on soit en présence d'une donnée personnelle dont le traitement est susceptible de porter atteinte à la personnalité du travailleur, il faut que l'information se rapporte à une personne (un travailleur) identifiée ou identifiable (cf. art. 3 let a LPD). Une personne est identifiée lorsqu'il ressort directement des informations détenues qu'il s'agit d'une personne déterminée et d'elle seule[36], par exemple lorsque le salaire est clairement mis en relation avec les nom et prénom d'un travailleur de l'entreprise. Par ailleurs, une personne est identifiable lorsque, par corrélation indirecte d'informations tirées des circonstances ou du contexte, il est possible de l'identifier[37], par exemple au moyen de son numéro AVS ou parce que le salaire est mis en relation avec un poste déterminé, telle que « directrice du service RH ». En revanche, une liste générale des salaires sans indication des noms ou fonctions des employés concernés ne constituera généralement par une donnée personnelle au sens de la LPD et de la protection de la personnalité des employés. Il en va de même de toute autre donnée anonymisée[38].

La LPD distingue des données personnelles ordinaires, les données sensibles, soit des informations confidentielles qu'il convient de traiter avec une discrétion accrue. La LPD

34 MEIER, N 2020.
35 BRUNNER/BÜHLER/WAEBER/BRUNNER, N 2 *ad* art. 328b CO, p. 154.
36 MEIER, N 431.
37 MEIER, N 432.
38 MEIER, N 436 ; ROSENTHAL, N 33 *ad* art. 328b CO, p. 733.

en donne une liste exhaustive dans laquelle ne figure pas le salaire des employés (cf. art. 3 let. c LPD). Il en résulte que le salaire d'un travailleur constitue une donnée personnelle ordinaire au sens de l'art. 3 let. a LPD[39].

La plupart des entreprises détiennent des fichiers concernant leurs employés (dossiers personnels « papier », fichiers électroniques), c'est-à-dire un ensemble de données organisé de telle manière que les données peuvent être recherchées par personne concernée (art. 3 let. g LPD). L'employeur en est généralement le « maître », soit la personne qui décide du but et du contenu du fichier (art. 3 let. i LPD).

La LPD donne un sens très large à la notion de « traitement » : il s'agit de toute opération relative à des données personnelles quels que soient les moyens et procédés utilisés : collecte, conservation, utilisation, modification, communication, archivage ou destructions de données (cf. art. 3 let. c LPD). Le législateur a choisi une liste exemplative et volontairement large, dans le but de couvrir toute opération portant sur des données personnelles[40]. En outre, il a souhaité donner une définition spécifique à la notion de « communication » estimant qu'il s'agissait de la phase la plus dangereuse du traitement des données puisque ces dernières quittent la sphère de maîtrise de celui qui les a collectées[41]. Selon l'article 3 lettre f LPD, la « communication » est définie comme le fait de rendre des données personnelles accessibles, par exemple en autorisant leur consultation, en les transmettant ou en les diffusant.

Les règles relatives au traitement des données personnelles par les entités privées sont celles de la section 3 de la loi (art. 12 à 15 LPD). Selon l'art. 12 al. 1 LPD, quiconque traite des données personnelles ne doit pas porter une atteinte illicite à la personnalité des personnes concernées. L'alinéa 2 de l'article 12 LPD dresse une liste exemplative de ce qui est constitutif d'une atteinte à la personnalité. Personne n'est en droit notamment de traiter des données personnelles en violation des principes généraux de la protection des données définis aux articles 4, 5 al. 1 et 7 al. 1 LPD (let. a) ou contre la volonté expresse de la personne concernée, sans motifs justificatifs (let. b).

En conclusion, les données salariales portant sur un travailleur identifié ou identifiable sont des données personnelles au sens de la législation sur la protection des données dont le traitement par l'employeur constitue en principe une atteinte à la personnalité du travailleur.

39 CRAMER, p. 1472 ; MEIER, N 475.
40 MEIER, N 521.
41 MEIER, N 535.

2. Motifs justificatifs

Nous avons vu que tout traitement (collecte, conservation, communication) d'un salaire par l'employeur constitue une source potentielle d'atteinte illicite à la personnalité du travailleur concerné. Selon les articles 28 al. 2 CC et 13 al. 1 LPD, qui sont similaires, une atteinte à la personnalité est illicite, à moins qu'elle ne soit justifiée par le consentement de la victime, par un intérêt prépondérant privé ou public, ou par la loi.

Après avoir exposé le système (**a**), nous traiterons des trois catégories de motifs justificatifs admises, à savoir une base légale (**b**), un intérêt prépondérant privé ou public (**c**) et le consentement du travailleur (**d**).

a) Système général

La question de déterminer à quelles conditions un employeur est autorisé à traiter des données personnelles de ses employés fait débat. Il faut dire que la portée de l'art. 328b CO, qui est une disposition semi-impérative (cf. art. 362 CO), est controversée[42]. Selon certains auteurs, cette disposition légale aurait essentiellement pour fonction de concrétiser en droit du travail les principes de proportionnalité (cf. art. 4 al. 2 LPD) et de finalité (cf. art. 4 al. 3 LPD) inscrits dans la loi sur la protection des données[43]. Selon d'autres auteurs, l'article 328b CO aurait, au contraire, une importance matérielle considérable : il poserait comme principe que tout traitement de données par l'employeur est en principe illicite, sauf s'il est couvert par les deux catégories de motifs justificatifs prévus dans la disposition elle-même (données portant sur les aptitudes du travailleur à remplir son emploi ou nécessaires à l'exécution du contrat de travail)[44].

De notre point de vue, il résulte du système général de protection de la personnalité des individus (cf. art. 28 al. 2 CC et art. 13 al. 1 LPD), ainsi que de la pratique, que l'employeur doit pouvoir se prévaloir des motifs justificatifs usuels, à savoir, une base légale, un intérêt prépondérant privé ou public ou le consentement du travailleur[45]. Par voie de conséquence, l'art. 328b CO ne constitue pas une norme d'interdiction et les deux motifs justificatifs qu'elle prévoit ne sauraient être considérés comme exhaustifs. Il convient finalement de s'en tenir à l'avis du Tribunal fédéral, selon lequel les données personnelles couvertes par l'art. 328b CO « bénéficient de la présomption légale qu'elles ne portent pas atteinte à la personnalité du travailleur »[46].

---

42 Pour un résumé de la controverse, cf. CRAMER, pp. 1472-1473 et ROSENTHAL, pp. 723 ss.

43 Cf., par exemple, MEIER, pp. 650 ss.

44 Cf., par exemple, STREIFF/VON KAENEL/RUDOLPH, N 3 *ad* art. 328b CO, pp. 579-580.

45 PORTMANN/RUDOLPH, N 25-28 *ad* art. 328b CO, pp. 1964-1965.

46 ATF 130 II 425, c. 3.3.

b) Base légale

La loi peut ordonner un traitement de données, le permettre ou le présupposer[47]. Lorsque la loi sert de motif justificatif, cela signifie que le législateur a procédé lui-même, à titre préalable, à une pesée des intérêts entre ceux de l'auteur de l'atteinte et ceux du lésé[48]. Il existe plusieurs dispositions légales qui autorisent, voire obligent, l'employeur à collecter, conserver ou communiquer à des tiers, à l'intérieur ou à l'extérieur de l'entreprise, des données relatives aux salaires de ses employés. Nous en donnerons quelques exemples.

aa) Données nécessaires à l'exécution du contrat de travail

Selon l'article 328b CO, l'employeur peut notamment traiter les données de ses employés qui « sont nécessaires à l'exécution du contrat de travail ». Il s'agit de toutes les données qui sont objectivement et matériellement nécessaires à l'exécution du contrat de travail[49]. L'article 328b CO constitue la principale base légale autorisant l'employeur à traiter des données salariales de ses employés.

En effet, pour remplir correctement ses obligations légales ou conventionnelles, l'employeur va nécessairement collecter, conserver et communiquer des informations relatives aux salaires de ses employés, ne serait-ce que pour calculer le montant du salaire brut, opérer les déductions fiscales, verser le salaire sur le compte bancaire de l'employé, établir les fiches de salaires ou encore les attestations annuelles de salaire. En application des dispositions légales applicables, l'employeur doit également communiquer les informations salariales pertinentes à diverses instances ou autorités, comme les institutions d'assurances sociales ou privées, les autorités fiscales, pénales et de poursuites, les inspections cantonales du travail ou encore les commissions tripartites et paritaires compétentes[50].

Deux décisions peuvent être citées dans ce contexte. Ainsi, selon le Préposé fédéral à la protection des données, si les données relatives aux salaires des travailleurs d'une entreprise déployant son activité en Suisse et ayant des relations avec l'étranger peuvent être communiquées aux autorités fiscales d'un autre pays conformément au droit applicable, alors l'article 328b CO ne s'oppose pas à une telle communication[51]. Par

---

47 MEIER, N 1601.

48 MEIER, N 1600.

49 MEIER, N 2046.

50 CRAMER, pp. 1477-1478 ; PORTMANN/RUDOLPH, N 9 *ad* art. 328b CO, p. 1962 ; ROSENTHAL, N 41 *ad* art. 328b CO, pp. 737 ss ; STREIFF/VON KAENEL/RUDOLPH, N 6 *ad* art. 328b CO, pp. 582-583. Sur la communication des données salariales aux commissions paritaires, cf. la contribution de STAUFFER dans le présent ouvrage, pp. 343 ss.

51 Préposé fédéral à la protection des données, décision du 7 mars 1995, *in* : JAAC 59.31.

ailleurs, dans un arrêt récent destiné à la publication aux ATF, le Tribunal fédéral a précisé que les employeurs étaient obligés de communiquer aux commissions tripartites instituées pour lutter contre le dumping salarial (cf. art. 360a et 360b CO) divers documents relatifs aux conditions salariales et aux conditions de travail de leurs employés (contrat de travail, décomptes de salaires et de temps de travail)[52].

Certains traitements ne sont, en revanche, pas couverts par l'article 328b CO et constituent donc, à défaut d'autres motifs justificatifs, une atteinte illicite à la personnalité du travailleur ou du postulant. Ainsi, lorsqu'il est mentionné en référence dans un dossier de postulation, l'employeur (actuel ou ancien) n'a pas à communiquer le montant du salaire du postulant au nouvel employeur potentiel[53]. De même, un employeur n'est en principe pas en droit de demander au postulant le montant de son (ancien) salaire lors de l'entretien d'embauche[54]. Quant à la communication des salaires à un acquéreur potentiel de la société dans le cadre d'une *due diligence*, elle ne paraît pas couverte par l'article 328b CO, mais par d'autres motifs justificatifs[55].

bb) Externalisation

La délégation de traitement (*outsourcing*) est autorisée, mais soumise à des conditions spécifiques. Le cas se présente lorsque l'employeur externalise la gestion des salaires, voire de l'ensemble des ressources humaines. Selon la LPD, l'externalisation d'un traitement de données est admise aux conditions cumulatives suivantes : la délégation se fonde sur une convention entre l'employeur et le mandataire ; celui-ci ne procède qu'à des traitements que l'employeur lui-même serait en droit de faire (en l'occurrence, selon l'art. 328b CO) ; aucune obligation légale ou contractuelle de garder le secret n'interdit le traitement ; les principes généraux de la protection des données sont respectés (cf. art. 10a LPD)[56]. La communication de données personnelles à l'étranger est soumise à des conditions particulières (cf. art. 6 LPD)[57]. Elle est en principe interdite, sauf garanties spécifiques, lorsque la législation du pays concerné n'assure pas une protection adéquate en matière de protection des données[58].

---

52 TF 2C_625/2016 du 12 décembre 2016, c. 3.

53 AUBERT, Protection, p. 154 ; CRAMER, pp. 1478-1479 ; MEIER, N 2085.

54 AUBERT, Protection, p. 154 ; CRAMER, p. 1479 ; MEIER, N 2090 ; STREIFF/VON KAENEL/RUDOLPH, N 10 *ad* art. 328b CO, p. 595. D'un avis contraire : REHBINDER/STÖCKLI, N 36 *ad* art. 320 CO, p. 96.

55 Sur cette question, cf. dans le présent ouvrage la contribution détaillée de CARRON/WENIGER, pp. 111 ss.

56 Sur ces questions, cf. MEIER, pp. 420 ss ; STREIFF/VON KAENEL/RUDOLPH, N 10b *ad* art. 328b CO, pp. 604-605.

57 Cf. MEIER, pp. 436 ss.

58 Sur ces questions, cf. la contribution de FLÜCKIGER dans le présent ouvrage, pp. 15 ss.

Dans le cas d'un groupe de sociétés, la société mère ne peut déléguer le traitement à une succursale ou à une autre société du même groupe (ou vice-versa) que si les conditions de l'art. 10a LPD sont remplies[59]. Par ailleurs, si la société mère a son siège en Suisse et qu'elle délègue le traitement de ses données à une filiale à l'étranger, les règles relatives à la communication transfrontalière de données personnelles devront être observées (cf. art. 6 al. 1 et al. 2 let. g LPD)[60].

cc) Calcul de la participation aux bénéfices

Le contrat de travail peut prévoir que l'employé a droit à une participation à une part du bénéfice ou du chiffre d'affaires ou qu'il participe d'une autre manière au résultat de l'exploitation[61]. La part due à l'employé est calculée sur la base du résultat de l'exercice annuel, déterminée conformément aux prescriptions légales et aux principes commerciaux généralement reconnus (art. 322a al. 1 CO).

Dans une telle situation, la loi impose à l'employeur à fournir les renseignements nécessaires au travailleur ou à un expert désigné en commun par les parties ou par le juge ; il fait également obligation à l'employeur d'autoriser le travailleur à consulter les livres de comptabilité dans la mesure nécessaire (art. 322a al. 2 CO). En outre, lorsqu'une participation aux bénéfices est convenue, l'art. 322 al. 3 CO oblige l'employeur à remettre une copie du compte de pertes et profits de l'exercice annuel au travailleur qui le demande.

Le Tribunal fédéral a jugé que la consultation de la comptabilité, garantie par l'art. 322a CO, impliquait la divulgation à l'employé concerné du revenu des autres travailleurs au service de l'employeur[62]. Ce traitement de données n'est pas nécessaire à l'exécution des contrats de travail des autres travailleurs. Il n'est donc pas couvert par l'article 328b CO et constitue un motif justificatif légal supplémentaire.

dd) Sociétés cotées en bourse

Il est aujourd'hui admis que la transparence constitue l'un des piliers du droit des sociétés, car elle permet la recherche d'un certain équilibre entre les intérêts des actionnaires, de la société, des travailleurs et des tiers[63]. Le droit suisse tend à consacrer une certaine transparence des indemnités versées aux dirigeants des sociétés.

C'est ainsi que les premières prescriptions sur la transparence des indemnités du conseil d'administration et de la direction générale des sociétés cotées sont entrées en vigueur le 1er janvier 2007 (cf. art. 663bis CO). Ces règles ont été complétées suite à l'acceptation de

59 DUNAND, N 22 *ad* art. 328b CO, p. 324.
60 MEIER, N 1270 et 1391 ss.
61 DANTHE, N 1 *ad* art. 322a CO, p. 147.
62 TF 4A_195/2010 du 8 juin 2010, c. 2.2.
63 URBEN, pp. 262-263.

l'initiative « contre les rémunérations abusives » qui a institué un nouvel article 95 al. 3 dans la Constitution fédérale. Afin de réaliser provisoirement le mandat constitutionnel, le Conseil fédéral a adopté une ordonnance contre les rémunérations abusives dans les sociétés cotées en bourse (ORAb), entrée en vigueur le 1er janvier 2014. L'ordonnance s'applique aux sociétés anonymes au sens des articles 620 à 762 du CO dont les actions sont cotées en bourse en Suisse ou à l'étranger (art. 1 al. 1 ORAb). Les règles de l'ORAb abrogent « de fait » certaines dispositions du droit de la société anonyme, durant la durée de la validité de l'ordonnance[64].

L'article 13 al. 1 ORAb prescrit que le conseil d'administration doit établir annuellement un rapport de rémunération écrit dans lequel doivent notamment être indiquées toutes les indemnités que la société a versées directement ou indirectement au conseil d'administration, à la direction et au conseil consultatif (cf. art. 14 ORAb). L'organe de révision vérifie si le rapport est conforme aux prescriptions légales et à celles de l'ORAb (art. 17 ORAb). Enfin, dans le but d'accroître le contrôle des actionnaires sur les rémunérations allouées aux dirigeants de la société, l'assemblée générale doit voter annuellement, de manière contraignante et séparée pour le conseil d'administration, la direction et le conseil consultatif, les montants globaux qui leur sont accordés (art. 18 al. 1 et 3 ORAb)[65].

Ces prescriptions qui obligent l'employeur à rendre publique la rémunération des dirigeants sont évidemment (absolument) impératives et priment les dispositions contraires du CO (art. 1 al. 2 ORAb)[66]. Elles constituent un motif justificatif légal de l'atteinte à la personnalité des personnes concernées[67].

Notons encore que lors de sa séance du 23 novembre 2016, le Conseil fédéral a transmis au Parlement un projet de révision du droit de la société anonyme qui prévoit d'intégrer dans le code des obligations les dispositions de l'ORAb. Le projet vise aussi à compléter le droit actuel sur certains points dans le but de renforcer la sécurité du droit et les droits des actionnaires et de mettre en œuvre certains aspects de l'initiative populaire sur les rémunérations abusives. Seront ainsi interdites les primes d'embauche ne compensant pas un désavantage financier établi et les indemnités découlant d'une interdiction de faire concurrence qui n'est pas justifiée par l'usage commercial. Le montant de ces indemnités sera aussi limité. Si les actionnaires votent de manière prospective sur les rémunérations

64 URBEN, p. 10.

65 WYLER/HEINZER, p. 145.

66 L'article 28 ORAb prévoit cependant une règle transitoire : « Les contrats de travail existant au moment de l'entrée en vigueur de la présente ordonnance doivent être adaptés dans un délai de deux ans à partir de cette date. Passé ce délai, la présente ordonnance est applicable à tous les contrats de travail ».

67 CRAMER, p. 1473.

variables des cadres supérieurs, ils devront après coup aussi voter à titre consultatif sur le rapport de rémunération. Enfin, la procédure pour intenter une action en restitution de rémunérations injustifiées sera simplifiée[68].

c) Intérêt prépondérant privé ou public

L'employeur est autorisé à communiquer le salaire d'un employé à un tiers lorsqu'il peut invoquer l'existence d'un intérêt prépondérant privé ou public propre à justifier une telle communication (art. 28 al. 2 CC et 13 al. 1 LPD). Un intérêt prépondérant privé existe lorsque le sacrifice qui est imposé à la victime est jugé inférieur à l'avantage que peut en retirer une autre personne, physique ou morale[69]. Quant à l'intérêt public, il existe lorsqu'il profite à une pluralité d'autres personnes ou à la collectivité[70]. Dans les relations entre privés, l'intérêt public vient en général en soutien d'un intérêt privé prépondérant[71]. En cas de contestation, le juge devra procéder à une pondération des intérêts en présence, à savoir l'intérêt de la victime à ne pas subir d'atteinte à sa personnalité et celui dont se prévaut l'auteur pour y porter atteinte[72]. Le législateur a dressé une liste non exhaustive d'intérêts prépondérants de l'auteur du traitement qui doivent entrer en considération dans l'examen du juge (art. 13 al. 2 LPD)[73]. La pesée des intérêts se fera toutefois au regard de l'ensemble des circonstances (art. 4 CC)[74]. L'atteinte ne sera considérée comme justifiée que si le juge parvient à la conclusion que l'intérêt invoqué par l'auteur est prépondérant par rapport à celui de la victime[75].

En matière de communication des données salariales, les cas les plus intéressants surviennent lorsqu'un employé demande à son employeur de lui transmettre le montant du salaire de certains collègues en vue de faire valoir des prétentions ou dans le cadre d'une procédure en justice. L'employeur a tendance à s'opposer à une telle demande en arguant de l'intérêt des employés concernés à la protection de leur personnalité, ainsi que de son propre intérêt au respect des obligations qui lui incombent en ce domaine (cf. art. 328 et 328b CO). Nous disposons en la matière de deux jurisprudences du Tribunal fédéral qui concernent, d'une part, la participation aux bénéfices, et d'autre part, le droit au bonus. Les règles posées dans ces arrêts nous paraissent pouvoir être étendues à d'autres

---

68 Communiqué du Conseil fédéral du 23 novembre 2016 intitulé : « Modernisation du droit de la société anonyme », lu sur le site de l'Office fédéral de la justice : www.bj.admin.ch > Actualité > News > 2016 (site consulté le 8 janvier 2017).

69 JEANDIN, N 79 *ad* art. 28 CC, p. 263.

70 JEANDIN, N 80 *ad* art. 28 CC, p. 263.

71 MEIER, N 1614.

72 JEANDIN, N 78 *ad* art. 28 CC, p. 263.

73 MEIER, N 1631.

74 MEIER, N 1628.

75 JEANDIN, N 78 *ad* art. 28 CC, p. 263.

prétentions, notamment celles qui se fondent sur le principe de l'égalité salariale entre les sexes.

aa) Participation aux bénéfices

Dans le cadre d'une procédure relative à un médecin spécialiste FMH en radiologie qui réclamait une participation aux bénéfices (art. 322a CO), un juge cantonal a ordonné à l'employeur de produire les comptes de pertes et profits, les bilans et le décompte des participations au bénéfice accordées aux divers salariés durant une période de 7 ans (de 2001 à 2008), avec les dates de chaque paiement desdites indemnités. L'employeur a interjeté un recours en matière civile auprès de Tribunal fédéral dans lequel il sollicitait l'annulation de l'ordonnance du juge. L'employeur invoquait l'intérêt des autres salariés à ce que leur salaire reste confidentiel, ainsi que son propre intérêt à prévenir le risque que la connaissance des revenus des collaborateurs facilite un éventuel débauchage par des tiers[76].

Effectuant implicitement une pesée des intérêts en présence, le Tribunal fédéral a rejeté les arguments de l'employeur. S'agissant du risque de débauchage, notre Haute Cour l'a jugé « assez théorique dès lors qu'on ne voit pas ce qui empêcherait des collaborateurs abordés par des employeurs potentiels de divulguer eux-mêmes leur revenu »[77]. Quant à l'obligation de l'employeur de protéger et respecter la personnalité de ses employés, elle ne fait pas obstacle, selon le Tribunal fédéral, à la divulgation des revenus de ces derniers. En effet, dans le cadre d'une procédure judiciaire entre employeur et travailleur dans laquelle le revenu des autres travailleurs au service de l'employeur est pertinent pour le jugement à rendre, l'employeur ne peut refuser de fournir ces données[78]. L'intérêt privé du médecin a donc été considéré comme prépondérant.

Il résulte de ce qui précède que si les données contenues dans la comptabilité sont nécessaires à la résolution de la cause, l'employeur ne peut s'opposer à leur production. Il pourra toutefois réclamer que certaines parties des pièces comptables, sans lien avec le litige ou devant demeurer confidentielles, soient caviardées[79].

bb) Bonus

Suite à une demande en justice d'un employé qui réclamait la condamnation de son employeur à lui verser des montants importants au titre de bonus, le Tribunal des prud'hommes du canton de Genève a enjoint l'employeur de produire les certificats de

76 TF 4A_195/2010 du 8 juin 2010, c. 2.
77 TF 4A_195/2010 du 8 juin 2010, c. 2.3.
78 TF 4A_195/2010 du 8 juin 2010, c. 2.2.
79 DIETSCHY, N 637, pp. 302-303.

salaire et/ou les lettres ou documents attestant le montant du bonus et sa méthode de calcul s'agissant de cinq collaborateurs de l'entreprise. La Chambre des prud'hommes de la Cour de justice genevoise a rejeté le recours formé par l'employeur contre cette décision. Ce dernier a interjeté un recours en matière civile auprès du Tribunal fédéral. L'employeur a fondé son refus de communiquer les documents litigieux sur l'article 163 CPC et invoqué la sphère privée de ses employés dont il entendait protéger les droits de la personnalité[80].

On rappellera que, en vertu de l'article 163 al. 1 CPC, une partie peut refuser de collaborer lorsque l'administration des preuves pourrait exposer un de ses proches au sens de l'art. 165 à une poursuite pénale ou engager sa responsabilité civile (lettre a) ou lorsque la révélation d'un secret pourrait être punissable en vertu de l'art. 321 du Code pénal ; les réviseurs sont exceptés ; l'art. 166 al. 1 let. b *in fine* est applicable par analogie (lettre b). Quant à l'art. 163 al. 2 CPC, il prévoit que les dépositaires d'autres secrets protégés par la loi peuvent refuser de collaborer s'ils rendent vraisemblable que l'intérêt à garder le secret l'emporte sur l'intérêt à la manifestation de la vérité.

L'arrêt rendu par le Tribunal fédéral dans cette affaire de bonus est intéressant en ce qu'il confirme et complète les principes dégagés dans l'arrêt que nous venons d'évoquer sur la participation aux bénéfices. Quatre éléments sont à relever. Premièrement, dès lors que la loi sur la protection des données ne s'applique pas aux procédures civiles pendantes (cf. art. 2 al. 2 let. c LPD), la question de la communication de données relève de l'art. 163 CPC. Les « règles spéciales de la procédure assurent déjà suffisamment la protection de la personnalité et il s'agit d'éviter un conflit de normes »[81]. Deuxièmement, le raisonnement tenu dans l'arrêt sur la participation aux bénéfices « s'applique mutatis mutandis dans la présente affaire, où la question des bonus touchés par d'autres collaborateurs importe pour l'issue du litige »[82]. Troisièmement, il n'est pas nécessaire de déterminer si les documents litigieux sont « protégés par la loi » au sens de l'art. 163 al. 2 CPC, car même si tel devait être le cas, il faudrait de toute manière admettre un intérêt prépondérant de l'employé à la manifestation de la vérité[83]. Quatrièmement, enfin, dans un procès en paiement d'un bonus, les juges n'ont pas besoin d'éclaircir au préalable la question du droit au bonus avant d'ordonner la production des titres pertinents[84].

cc) Egalité salariale selon la LEg

La loi sur l'égalité prohibe les discriminations salariales qui surviennent lorsque des différences de salaire reposant sur des circonstances qui découlent de l'appartenance à un

80 TF 4A_63/2016 du 10 octobre 2016. Pour un commentaire détaillé de cet arrêt, cf. WITZIG.
81 TF 4A_63/2016 du 10 octobre 2016, c. 5.2.2.
82 TF 4A_63/2016 du 10 octobre 2016, c. 5.4.
83 TF 4A_63/2016 du 10 octobre 2016, c. 5.4.
84 TF 4A_63/2016 du 10 octobre 2016, c. 5.4.

sexe ne sont pas matériellement justifiées par le travail lui-même[85]. L'employée qui subit une discrimination salariale à raison du sexe peut réclamer à son employeur le salaire dû (cf. art. 3 et 5 al. 1 let. d LEg), soit la différence entre le salaire effectivement perçu et le salaire exempt de discrimination[86]. L'existence d'une discrimination est présumée pour autant que la personne qui s'en prévaut la rende vraisemblable (art. 6 LEg).

Il va de soi que les jurisprudences précitées relatives à la participation aux bénéfices et au bonus s'appliquent aux prétentions salariales fondées sur la loi sur l'égalité. Il en résulte selon nous qu'une employée est en droit de demander à son employeur de lui communiquer le montant des salaires versés à des collègues masculins qui fournissent un travail comparable ou de valeur égale. Dans le cadre d'une procédure judiciaire, l'intérêt de l'employée à la communication de ces informations devrait être considéré comme prépondérant.

Si l'on se base sur l'arrêt du Tribunal fédéral en matière de bonus, l'employée est en droit de solliciter ces informations sans qu'elle ait besoin de prouver, et ni même de rendre vraisemblable, qu'elle a effectivement droit au paiement de la différence salariale. On précisera ici que l'application de l'art. 6 LEg (allégement du fardeau de la preuve) doit intervenir à l'issue de la procédure lorsque tous les moyens de preuve ont été administrés. C'est en effet à ce moment-là que le juge devra déterminer, sur la base des faits établis, s'il considère qu'une discrimination a été rendue vraisemblable et, si tel est le cas, s'il existe des éléments objectifs non discriminatoires permettant de justifier la différence de traitement[87]. D'ailleurs, dans ce cadre l'employeur peut lui-même se prévaloir d'un intérêt privé prépondérant à révéler spontanément le salaire de certains de ses employés, afin de convaincre le juge que la demanderesse n'a pas été victime d'une discrimination salariale[88].

On peut enfin se demander si la communication par l'employeur à une employée des salaires de collègues de travail masculins ne repose pas également sur l'intérêt public, garanti à l'article 8 alinéa 3 de la Constitution fédérale, de l'égalité salariale entre les sexes ? En tous les cas, on relèvera que le Conseil fédéral souhaite une plus grande transparence en la matière. C'est ainsi qu'en date du 26 octobre 2016, il a chargé le Département fédéral de justice et police de préparer un projet de loi d'ici l'été 2017 dans lequel il devra être prévu que les entreprises qui emploient au moins cinquante personnes auront l'obligation d'analyser tous les quatre ans les salaires qu'elles versent ; il est aussi

85 GIRARDIN, N 22 *ad* art.3 LEg, p. 78.
86 GIRARDIN, N 11 *ad* art. 3 LEg, p. 74.
87 BRUCHEZ, p. 181 ; WYLER, N 10 *ad* art. 6 LEg, pp. 152-153.
88 CRAMER, pp. 1481-1482.

prévu qu'un organe de contrôle externe vérifie le bon déroulement de l'analyse et rende compte du résultat de son examen à la direction de l'entreprise[89].

d) Consentement

Le consentement de la victime peut constituer un motif justificatif de l'atteinte à la personnalité (art. 28 al. 2 CC et 13 al. 1 LPD). Le consentement constitue une manifestation de volonté, un acte juridique unilatéral, qui n'est soumis à aucune forme particulière[90]. La personne qui a donné le consentement à une atteinte a le droit de le révoquer en tout temps, ce à quoi elle ne peut renoncer à l'avance[91].

L'ordre juridique contient des règles qui limitent la possibilité de la victime de consentir à une atteinte. Ainsi, l'article 27 alinéa 2 CC prévoit que nul ne peut aliéner sa liberté, ni s'en interdire l'usage dans une mesure contraire aux lois ou aux mœurs (protection contre les engagements excessifs). Par ailleurs, lorsque son consentement est requis pour le traitement de données personnelles la concernant, la personne concernée ne consent valablement que si elle exprime sa volonté librement et après avoir été dûment informée ; c'est le principe du consentement libre et éclairé (art. 4 al. 5 LPD)[92].

Dans le cadre des relations de travail, il convient d'apprécier strictement la portée du consentement du travailleur en raison du lien de subordination entre l'employeur et l'employé qui peut engendrer une dépendance psychologique et économique[93]. Plus l'acte auquel le travailleur consent est éloigné du cadre de l'article 328b CO et plus on se montrera réticent à admettre la validité du consentement[94].

Par ailleurs, il faut rappeler que les articles 328 et 328b CO constituent des dispositions relativement impératives, c'est-à-dire auxquelles il ne peut être dérogé au détriment du travailleur (art. 362 CO). Il en résulte, selon nous, qu'un travailleur ne peut consentir à un traitement de données allant au-delà du cadre de l'art. 328b CO, que dans les limites de l'article 341 CO, selon lequel le travailleur ne peut renoncer, pendant la durée du contrat et durant le mois qui suit la fin de celui-ci, aux créances résultant de dispositions impératives de la loi ou d'une convention collective. Pour que le consentement du

---

89 Communiqué du Conseil fédéral du 26 octobre 2016 intitulé: « Une avancée vers l'égalité salariale : le Conseil fédéral veut un message d'ici à l'été 2017 », lu sur le site de l'Office fédéral de la justice : www.bj.admin.ch > Actualité > News > 2016 (site consulté le 8 janvier 2017).

90 JEANDIN, N 73 *ad* art. 28 CC, p. 262.

91 JEANDIN, N 75 *ad* art. 28 CC, p. 262.

92 MEIER, pp. 316 ss.

93 Arrêt de la Cour d'appel civile du Tribunal cantonal vaudois du 7 juillet 2016, cause PT13.05374, c. 5.2.2. Voir également WYLER/HEINZER, p. 310.

94 MEIER, N 2057.

travailleur soit valable, il faut donc qu'il porte sur une atteinte qui puisse être considérée comme étant dans son propre intérêt[95]. Un tel intérêt existera, par exemple, lorsque l'employé demande à son employeur de communiquer directement à un bailleur ou un prêteur potentiel des indications sur son salaire mensuel ou annuel (remise d'une attestation de salaire)[96].

3. Respect des principes généraux

L'existence d'un motif justificatif ne suffit pas à rendre licite un traitement des données par l'employeur[97]. Encore faut-il que le traitement soit conforme aux principes généraux résultant des articles 4, 5 al. 1 et 7 al. 1 LPD[98]. Comme nous l'avons vu, la violation de ces principes fait présumer une atteinte à la personnalité du travailleur (cf. art. 12 al. 2 let. a LPD)[99]. Le Tribunal fédéral a lui-même souligné que le procédé utilisé devait respecter la personnalité des travailleurs et observer les principes généraux du droit, en particulier ceux de la bonne foi et de la proportionnalité[100].

Dans l'ordre, la LPD énumère les principes suivants : licéité (art. 4 al. 1 LPD) ; bonne foi (art. 4 al. 2 LPD) ; proportionnalité (art. 4 al. 2 LPD) ; finalité (art. 4 al. 4 LPD) ; reconnaissabilité (art. 4 al. 4 LPD) ; exactitude (art. 5 al. 1 LPD) et sécurité (art. 7 al. 1 LPD)[101].

Nous évoquerons ici trois questions en lien avec la protection de la confidentialité du salaire : la limitation de l'accès aux données salariales (**a**), la protection des données salariales contre le vol (**b**) et la communication des données salariales à une société commerciale (**c**).

a) Limitation de l'accès aux données salariales

Tout traitement des données doit respecter le principe de la proportionnalité (art. 4 al. 2 LPD). Principe fondamental du droit public, consacré à l'article 36 alinéa 3 de la Constitution fédérale, le principe se compose de trois volets : la règle d'aptitude ou d'adéquation, la règle de nécessité et la règle de proportionnalité au sens étroit. Dans notre contexte, on en déduira que l'employeur ne peut collecter et traiter que les données qui

---

95 DUNAND, N 32 *ad* art. 328b CO, p. 327 ; PORTMANN/RUDOLPH, N 26 *ad* art. 328b CO, pp. 1964-1965.

96 CARRUZZO, N 17 *ad* art. 328b CO, p. 334 ; CRAMER, p. 1480.

97 DUNAND, N 34 *ad* art. 328b CO, p. 328.

98 MEIER, N 2055 ; PORTMANN/RUDOLPH, N 23 *ad* art. 328b CO, p. 1964.

99 ATF 136 II 508, c. 5, *in* : JdT 2011 II 446.

100 ATF 130 II 425, c. 3.3.

101 Pour une présentation de ces principes, cf. dans le présent ouvrage la contribution de FLÜCKIGER, pp. 10 ss.

sont aptes et objectivement nécessaires pour atteindre le but poursuivi, pour autant que le traitement demeure dans un rapport raisonnable entre le résultat recherché et le moyen utilisé, tout en préservant le plus possible le droit des personnes concernées[102].

Afin de limiter l'atteinte à la personnalité des employés, l'employeur doit s'assurer que le moins grand nombre possible de personnes aillent accès aux données salariales dans l'entreprise. Un tel accès devrait être limité aux personnes devant nécessairement manipuler ces données pour le calcul et le versement du salaire, ainsi qu'aux supérieurs hiérarchiques dans la ligne verticale directe[103]. En aucun cas, les collaborateurs ne doivent avoir accès aux données personnelles de leurs collègues.

b) Protection des données salariales contre le vol

Selon l'art. 7 al. 1 LPD, les données personnelles doivent être protégées contre tout traitement non autorisé par des mesures organisationnelles et techniques appropriées (principe de sécurité)[104]. Les mesures à prendre sont détaillées aux articles 8 et 9 OLPD. Les composantes de la sécurité comprennent trois aspects : la confidentialité (seuls des personnes légitimées ou des logiciels légitimés peuvent avoir accès aux données salariales) ; la disponibilité (l'information désirée doit être disponible en un lieu voulu, dans une forme voulue et à un moment voulu) ; l'intégrité (le contenu de l'information est protégé contre des manipulations humaines ou logicielles malveillantes)[105]. Ainsi, qu'ils figurent dans des dossiers ou registres « papier » ou électronique, l'employeur doit s'assurer que seules les personnes autorisées puissent avoir accès aux données salariales des employés et prendre les mesures adéquates pour que ces données ne puissent être volées.

c) Communication des données salariales à une société commerciale

Selon le principe de la finalité, les données personnelles ne doivent être traitées que dans le but qui est indiqué lors de leur collecte, qui est prévu par la loi ou qui ressort des circonstances (art. 4 al. 3 LPD). Il va de soi que l'employeur ne saurait communiquer le montant du salaire de ses employés à des sociétés commerciales pour permettre à celles-ci d'identifier leur capacité financière[106]. Une telle pratique serait autant dépourvue de tout

---

102 MEIER, N 666.

103 Sur la limitation d'accès aux données personnelles des travailleurs, cf. MONTAVON, p. 81 ; WYLER/HEINZER, p. 342.

104 Sur cette question, cf. la contribution de FANTI dans le présent ouvrage, pp. 235 ss.

105 MEIER, N 786.

106 MONTAVON, p. 81.

motif justificatif, qu'elle contreviendrait aux principes de la finalité du traitement et, plus généralement, de la bonne foi.

4. Réserve en faveur des lois sur la transparence

Enfin, il ne faut pas omettre de vérifier si la communication des données ne pourrait pas être ordonnée en vertu de la Loi fédérale sur le principe de la transparence dans l'administration du 17 décembre 2004[107], respectivement de la Convention intercantonale relative à la protection des données et à la transparence dans les cantons du Jura et de Neuchâtel du 9 mai 2012[108]. En effet, ces textes, bien que destinés avant tout à favoriser la transparence de l'administration, sont également susceptibles de s'appliquer à des entités privées.

Tel est le cas, en droit fédéral, des entités privées appelées à rendre des décisions (art. 2 al. 1 LTrans), mais uniquement pour les documents qui sont en relation directe avec la décision à prendre[109] ; ne sont en revanche pas visées les entités à qui des tâches administratives sont confiées au cas par cas[110]. En droit cantonal, le cercle des entités visées est plus large puisqu'il s'agit de celles qui accomplissent des tâches d'intérêt public (art. 2 let d CPDT-JUNE) ou dans lesquelles les collectivités publiques détiennent une participation majoritaire dans celles-ci (art. 2 let. e CPDT-JUNE).

Une entité privée qui se trouve d'une manière ou d'une autre en relation avec une collectivité publique, qu'elle soit chargée de l'exécution d'une tâche publique ou subventionnée par des deniers publics, doit donc s'assurer de son assujettissement ou non à la LTrans ou à l'équivalent de cette loi au niveau cantonal[111].

B. En droit de la fonction publique

1. Protection de la personnalité de l'agent public

Tout comme l'employeur privé, l'employeur public a le devoir de protéger la personnalité des agents à son service[112]. En effet, la protection de la sphère privée est garantie explicitement par l'art. 13 Cst. et, s'agissant de la communication de données concernant

---

107 LTrans, RS 152.3.

108 CPDT-JUNE, RSN 150.30.

109 ATAF 2015/43, c. 7.

110 ATAF 2015/43, c. 6.5.

111 Pour la mise en œuvre des dispositions sur la transparence, voir la contribution de WALTER dans le présent ouvrage, p. 75, ainsi qu'*infra* B. 2. a) iv.).

112 ATF 137 I 58, c. 4.2.3.

l'agent public, les notions de sphère privée et de protection de la personnalité concordent[113].

Dans le régime de la LPers, cette obligation a sa source à l'art. 4 al. 2 let. g LPers. De manière constante, les contours de cette obligation sont décrits au regard des devoirs découlant de l'art. 328 CO[114], conformément au renvoi de l'art. 6 al. 2 LPers.

En revanche, la LSt ne prévoit pas de disposition protégeant expressément la personnalité des fonctionnaires et employés du canton. Dans un tel cas de figure, en l'absence de disposition expresse, les art. 28ss CC et 328 CO devraient à notre sens trouver application à titre subsidiaire et par analogie, à titre de droit cantonal supplétif[115].

Par conséquent, tout comme dans le régime de travail de droit privé (voir *supra* A. 1. a), la rétribution des agents de la fonction publique constitue un élément de la personnalité des employés dont la confidentialité est protégée.

Il est vrai que la rétribution des agents publics peut dans une certaine mesure être déterminable : par le jeu de la fonction occupée et de l'échelle des traitements, le traitement maximal, voire minimal en droit cantonal, des agents publics se déduit de la loi ; il en va de même, en droit cantonal, des augmentations annuelles par échelon. Mais à l'intérieur de cette fourchette, les éléments qui permettent de fixer le salaire initial ainsi que, au plan fédéral, son évolution, relèvent à notre sens également de la sphère privée. En effet, le salaire respectivement le traitement sont fixés initialement en fonction de critères propres à l'agent public. De même, la progression salariale, en droit fédéral, dépend de l'évaluation personnelle de l'employé. Aussi, le fait que le salaire soit fixé de manière générale dans la loi ne signifie pas encore que le salaire de chaque agent public soit connu.

En outre, certaines rémunérations, en sus d'être déterminables, sont déclarées publiques de par la loi. Dans ce cas, c'est le législateur qui a, en amont, considéré que la publicité des rémunérations devait l'emporter sur la protection de la sphère privée.

Ainsi, l'art. 6a al. 4 et 5 LPers prévoit une publicité étendue voire totale pour le salaire des cadres du plus haut niveau hiérarchique des Chemins de fer fédéraux et d'autres entreprises et établissements de la Confédération,[116] mais aussi pour les entreprises sises en Suisse

---

113 ATAF 2013/50, c. 9.2.

114 TAF A-566/2015 du 24 août 2016, c. 4.2.2.3 ; TAF A-5276/2015 du 29 juin 2016, c. 4.3.1.3 ; TAF A-612/2015 du 4 mars 2016, c. 3.2 ; HELBLING, N. 44 *ad* art. 4 LPers.

115 TF 2A.770/2006 du 26 avril 2007, c. 3.2. Eg. TF 1C_394/2008 du 5 décembre 2008, c. 3.2. Plus nuancé, CDP.2016.191 (Cour de droit public du Tribunal cantonal, Neuchâtel, 24 octobre 2016), qui laisse la question ouverte tout en en niant une quelconque atteinte à la personnalité de l'agent public.

116 Notamment l'Institut fédéral de la propriété intellectuelle, Swissmedic, la Caisse nationale suisse d'assurance en cas d'accident, l'Inspection fédérale de la sécurité nucléaire, l'Autorité fédérale de

dont le capital et les voix sont détenus à titre majoritaire, directement ou indirectement, par la Confédération[117] : d'une part, le montant total des salaires ainsi que les autres conditions contractuelles avec ces personnes sont publics ; d'autre part, le salaire du président de la direction est mentionné individuellement. Cette publicité a été l'accessoire des mesures prises par la Confédération pour répondre à l'envolée du montant des rémunérations des cadres qui avait choqué l'opinion publique au début des années 2000 ; désormais, ces rémunérations sont fixées en tenant compte de l'ensemble des conditions politiques, économiques et sociales. La publicité qui s'y rapporte permet de restaurer la confiance dans les mesures prises[118].

De plus, selon l'art. 15 al. 6 LPers, le montant des salaires maximaux (prestations annexes comprises) à verser aux cadres du plus haut niveau hiérarchique de l'administration fédérale ainsi que les autres conditions contractuelles convenues avec ces personnes sont publics. Cette disposition est le pendant de l'art. 6a LPers pour les cadres de l'administration centrale, mais la correspondance entre ces deux dispositions n'est pas totale[119]. Par « cadres de plus haut niveau », on entend, selon la doctrine, les personnes dont la classe de salaire est de 34 à 38[120]. Ce qui est public, ce n'est pas le salaire effectivement versé à chaque cadre, mais la rémunération maximale à laquelle il peut prétendre conformément à la loi ou aux dispositions d'exécution de celle-ci. De la sorte, il n'est pas possible de déterminer, par le biais du salaire effectivement versé, la qualité du travail de la personne en cause. Le législateur a ainsi souhaité éviter une atteinte trop importante à la personnalité de ces employés[121].

Le Conseil fédéral transmet chaque année son Rapport sur le salaire des cadres à l'attention de la Délégation des finances des chambres fédérales et celui-ci est publié sur le site de l'Office fédéral du personnel[122].

surveillance des marchés financiers, l'Autorité fédérale de surveillance en matière de révision, Pro Helvetia, La Poste Suisse et les entreprises qu'elle contrôle : art.1 de l'Ordonnance sur la rémunération et sur d'autres conditions contractuelles convenues avec les cadres du plus haut niveau hiérarchique et les membres des organes dirigeants des entreprises et des établissements de la Confédération du 19 décembre 2003 (Ordonnance sur le salaire des cadres, RS 172.220.12).

117 Notamment RUAG Holding SA, Hôtel Bellevue-Palace Immobilien AG, SIFEM, Swiss Investment Fund for Emerging Markets, Postfinance SA, SKYGUIDE, la SSR.

118 Rapport sur le salaire des cadres, pp. 6973-6974.

119 MALLA, N 152 *ad* art. 15 LPers.

120 MALLA, N 152 *ad* art. 15 LPers.

121 MALLA, N 162 *ad* art. 15 LPers.

122 www.epa.admin.ch, sous la rubrique Documentation>Faits et chiffres>Rapports.

2. Protection des données et transparence

Pour ce qui est de la protection des données dans le droit de la fonction publique, il convient de distinguer la fonction publique fédérale de la fonction publique cantonale ou communale. En effet, la LPD s'applique aux seuls organes fédéraux (art. 2 al. 1 let. b. LPD), de sorte que c'est dans les textes de rang cantonal sur la protection des données que celle-ci s'exprime pour la fonction publique cantonale et communale. De même, les législations sur la transparence sont fédérale, respectivement cantonales.

a) Fonction publique fédérale (art. 27ss LPers, LPD et LTrans)

aa) Champ d'application de la LPD

Les organes fédéraux à qui la LPD s'applique sont l'autorité ou le service fédéral ainsi que la personne en tant qu'elle est chargée d'une tâche de la Confédération (art. 3 let. h. LPD). Il s'agit avant tout de toutes les entités qui composent l'administration fédérale centrale et décentralisée au sens de l'article 2 de la Loi sur l'organisation du gouvernement et de l'administration du 21 mars 1997[123] ainsi que les entités décentralisées au sens propre du terme[124]. Mais à notre sens, cela concerne également les entités du pouvoir législatif ou judiciaire en leur qualité d'employeur au sens de la LPers, à savoir les Services du Parlement (art. 2 al. 1 let. b LPers), le Tribunal administratif fédéral, le Tribunal pénal fédéral, le Tribunal fédéral des brevets (art. 2 al. 1 let. f LPers), le Tribunal fédéral (art. 2 al. 1 let. g LPers), le secrétariat de l'Autorité de surveillance du Ministère public de la Confédération (art. 2 al. 1 let. h LPers) et le Ministère public de la Confédération (art. 2 al. 1 let. i LPers).

Pour ces autorités fédérales, les règles relatives au traitement des données personnelles figurent dans la section 4 de la loi, soit aux art. 16 à 25bis LPD. Le principe général est que le traitement de données personnelles ne peut intervenir que s'il existe une base légale (au sens matériel[125]) et, en présence de données sensibles ou de profils de la personnalité, s'il existe une base légale formelle (art. 17 LPD) (**bb**). La communication de données personnelles ne peut intervenir que moyennant base légale ou sur la base de motifs justificatifs, sous réserve de motifs de refus (cc). Enfin, la communication peut intervenir à la suite d'une demande fondée sur la LTrans (**dd**). Nous examinerons ensuite les critères retenus par la jurisprudence pour la transmission d'informations financières relatives aux employés de la Confédération (**ee**) et évoquerons la question des rémunérations accessoires des agents publics (**ff**).

---

123 LOGA, RS 172.020. MAURER-LAMBROU/KUNZ, N 13 *ad* art. 2 LPD.
124 RUDIN, N 44-45 *ad* art. 3 LPD.
125 MUND, N 5 *ad* art. 17 LPD.

bb) Exigence d'une base légale. Extension de la notion de données sensibles ?

En droit de la fonction publique fédérale, les art. 27 et suivants LPers, l'art. 9 OPers ainsi que l'Ordonnance concernant la protection des données personnelles du personnel de la Confédération du 26 octobre 2011[126] sont les bases légales pertinentes.

L'art. 27 LPers est la base légale générale permettant le traitement des données personnelles des employés de la Confédération ; elle prend la forme d'une clause de délégation en faveur du Conseil fédéral. La réglementation d'exécution porte, notamment, sur les conditions du traitement des données sensibles et des profils de la personnalité dans la mesure où ce traitement est nécessaire au développement du personnel et où la personne y a donné son consentement écrit (art. 27 al. 2 let. b LPers) ; les profils de personnalité visés par cette disposition sont les assessments et tests de la personnalité[127] utilisés lors du recrutement, mais aussi, à notre sens, les évaluations du personnel en vue de l'évolution du salaire. La réglementation d'exécution concerne également le délai de conservation des données, l'organisation des systèmes informatiques de traitement des données et la sécurité des données (art. 27 al. 2 let. c LPers).

L'art. 27a LPers est la base légale permettant à la Confédération d'exploiter un système d'information concernant le personnel. Ce système, nommé BV PLUS (art. 8 OPDC), a pour but de permettre la gestion centrale et l'exploitation des données personnelles relatives aux employés de l'administration et en particulier de traiter les données relatives au salaire et de réaliser des évaluations, des simulations de budget et des planifications des frais de personnel (art. 27a al. 1 let. a et b LPers). L'alinéa 2 de l'art. 27a LPers énumère un certain nombre de données sensibles pouvant figurer dans le système d'information du personnel ; parmi celles-ci figurent les échelons d'évaluation fondés sur les évaluations personnelles (art. 27a al. 3 let. e LPers) ainsi que la saisie du salaire (art. 27a al. 3 let. h LPers). BV PLUS est sous la responsabilité de l'Office fédéral du personnel tandis que les unités administratives sont responsables du traitement des données (art. 15 al. 1 et 2 OPDC).

Par le jeu de ces dispositions et du principe *lex posterior derogat priori*, le salaire en droit de la fonction publique fédérale semble érigé en donnée sensible, étendant ainsi, potentiellement, le champ d'application de l'art. 3 let. c LPD. Tel n'est toutefois pas l'opinion du Tribunal administratif fédéral, qui considère que les données de nature financière ou organisationnelle entourant la relation de travail ne sont pas des données

126 OPDC, RS 172.220.111.4.
127 Message LPers, p. 1446.

sensibles requérant une protection accrue[128] et que l'art. 27a al. 1 let. h LPers n'a aucune pertinence dans l'analyse de l'art. 3 let. c LPD[129].

cc) La communication de données personnelles

La communication des données personnelles peut intervenir dans deux cas de figure. D'une part, une base légale l'exige ou le permet. En droit du personnel fédéral, les art. 7 et 11 OPDC régissent la communication des données à des tiers, fondée sur le consentement de la personne, respectivement le transfert des données non sensibles contenues dans BV PLUS à d'autres systèmes d'information.

D'autre part, la communication peut intervenir si l'une des quatre conditions alternatives suivantes est réalisée : le destinataire a absolument besoin de ces données pour accomplir sa tâche légale, la personne y a consenti, elle a rendu ses données accessibles à tout un chacun et ne s'est pas formellement opposée à la communication ou le destinataire rend vraisemblable que la personne concernée ne refuse son accord ou ne s'oppose à la communication que dans le but de l'empêcher de se prévaloir de prétentions juridiques ou de faire valoir d'autres intérêts légitimes (art. 19 al. 1 LPD).

Néanmoins, les organes fédéraux sont en droit de communiquer, sur demande, le nom, le prénom, l'adresse et la date de naissance d'une personne même si les conditions susmentionnées ne sont pas réalisées (art. 19 al. 2 LPD).

Enfin, la communication peut être refusée, restreinte ou assortie de charges si un intérêt public ou privé important l'exige, s'il existe une obligation légale de garder le secret ou si une disposition particulière relevant de la protection des données l'exige (art. 19 al. 4 LPD).

À ces conditions et pesée des intérêts s'ajoutent encore les exigences en matière de transparence de l'administration.

dd) Le principe de transparence

La contribution de M. WALTER dans le présent ouvrage étudie en détail la relation entre le principe de transparence et la protection des données[130].

On retient en substance que la LTrans fonde le droit général de toute personne de consulter des documents officiels et d'obtenir des renseignements sur leur contenu de la part des autorités. Le processus décisionnel de l'administration est rendu plus transparent dans le

128 TAF A-3609/2010 du 17 février 2011, c. 5.4.
129 TAF A-6738/2014 du 23 septembre 2015.
130 Cf. pp. 77 ss.

but de renforcer le caractère démocratique des institutions publiques de même que la confiance des citoyens dans les autorités, tout en améliorant le contrôle de l'administration[131]. Le principe de transparence contribue à la réalisation de la liberté d'information (art. 16 Cst.), au devoir de renseigner de la Confédération (art. 180 al. 2 Cst.) ainsi que, de manière indirecte, à la liberté des médias (art. 17 Cst.)[132].

La LTrans s'applique à l'ensemble de l'administration fédérale, définie selon l'art. 2 LOGA. Il s'agit de l'ensemble de l'administration subordonnée au Conseil fédéral, soit les départements et les offices ainsi que la Chancellerie fédérale. Le Conseil fédéral, en tant qu'autorité politique indépendante de l'administration, dont les délibérations ont lieu à huis clos, ne s'y trouve point soumis[133]. Mais la LTrans s'applique également aux organismes de droit privé chargés de rendre des décisions, de sorte que les intérêts publics poursuivis par cette loi sont également susceptibles d'entrer dans la pesée des intérêts alors même que la relation de travail relève du droit privé (voir *supra* A. 4.).

La loi prévoit le principe de l'accès aux documents (art. 6 LTrans) et les exceptions à celui-ci (art. 7 et 8 LTrans) et c'est à l'autorité, si elle décide de refuser l'accès à des documents officiels, de supporter le fardeau de la preuve destinée à renverser la présomption du libre accès aux documents officiels[134].

L'art. 9 LTrans est la disposition prévoyant la coordination entre les deux régimes de la transparence, présumée, et de la protection des données, en principe garantie. Si, lors de l'adoption de la LTrans, le législateur considérait que le droit à la protection des données personnelles devait par principe primer sur la transparence[135], on retient aujourd'hui qu'il n'y a pas de préséance de l'une sur l'autre[136].

L'art. 9 LTrans prévoit une procédure par étapes. Tout d'abord, les documents officiels contenant des données personnelles doivent être si possible rendus anonymes (art. 9 al. 1 LTrans). S'ils ne peuvent pas l'être, l'art. 19 LPD est applicable. L'anonymisation est notamment impossible si la demande d'accès porte expressément sur une personne déterminée nommée dans la requête ou parce que le caviardage nécessiterait un travail disproportionné[137].

131 ATF 136 II 399, c. 2.1 ; ATF 133 II 209, c. 2.3.1.
132 ATF 142 II 113, c. 3.1.
133 ATAF 2014/24, c. 3.1.
134 ATAF 2014/24, c. 3.1.
135 Message LTrans, p. 1857.
136 Dans ce sens, TAF A-4571/2015 du 10 août 2016, c. 7.2.2. Voir aussi la contribution de WALTER dans le présent ouvrage.
137 Message LTrans p. 1858.

Selon l'art. 19 al.1bis LPD, les organes fédéraux peuvent communiquer des données personnelles en vertu de la LTrans si les données concernées sont en rapport avec l'accomplissement de tâches publiques et si la communication répond à un intérêt public prépondérant[138]. Ainsi, l'art. 9 al. 2 LTrans en relation avec l'art. 19 al. 1bis LPD, commande de déterminer au cas par cas, après évaluation minutieuse des intérêts en présence, le type de données pouvant être publiées. Mais la divulgation de données personnelles à l'issue d'une pondération des intérêts ne signifie pas que ces données tombent automatiquement dans le domaine public ; cela veut seulement dire que dans les circonstances de l'espèce, un intérêt public à la transparence a prévalu[139].

Le principe de la transparence vient donc accentuer la pression sur la protection des données. Pour les salaires et d'autres éléments de rétribution des agents de la Confédération, cela s'exprime comme suit.

ee) Le salaire des employés de la Confédération

Bien que globalement déterminable en fonction des classes de salaire fixées par la loi, le salaire réel des employés de la Confédération est une donnée personnelle protégée par la loi. Il ne s'agit pas d'une donnée sensible, car, selon les termes du Tribunal administratif fédéral, elle est de nature purement financière et organisationnelle, de sorte qu'elle ne nécessite pas une protection accrue[140].

La pesée des intérêts est guidée par les éléments suivants :

Tout d'abord, on doit admettre qu'en raison de leur qualité d'agent public, les employés de l'État ne bénéficient pas de la même protection à leur droit à l'autodétermination informationnelle que les privés[141].

De plus, les personnes occupant des positions élevées au sein de la hiérarchie administrative doivent davantage s'accommoder de la publication de leurs données personnelles que les employés exerçant des fonctions subalternes[142].

En outre, en référence à l'art. 6 al. 2 OTrans, un intérêt public à la transparence est jugé prépondérant, par exemple, lorsque le droit d'accès à un document répond à un besoin particulier d'information de la part du public suite notamment à des événements

138 TAF A-3649/2014, c. 8.3.3.
139 TAF A-3649/2014, c. 8.3.4.
140 Voir *supra* bb.
141 TAF A- 6738/2014 du 23 septembre 2015, c. 5.1.3.1, et les références.
142 TAF A- 6738/2014 du 23 septembre 2015, c. 5.1.3.1; TAF A-3609/2010 du 17 février 2011, c. 4.4.

importants, en particulier des événements de nature politique ; il en va de même s'il s'agit de documents en rapport avec l'octroi d'avantages économiques importants[143].

Enfin, constitue également un intérêt public important celui de pouvoir s'assurer que les dispositions légales en matière de rémunération sont correctement appliquées[144].

Il découle de l'application de ces critères que le salaire des employés de la Confédération, dans ces circonstances, ne bénéficie pas d'une protection aussi intense que les salaires des employés du secteur privé.

Enfin, comme déjà relevé le salaire maximal possible des cadres du plus haut niveau hiérarchique de l'administration ainsi que le salaire effectif des présidents des directions des établissements et entreprises de la Confédération, sont déclarés publics de par la loi[145].

ff) Les activités accessoires des employés de la Confédération[146]

La problématique des activités accessoires se pose différemment : ce n'est pas l'usage des deniers publics que l'on vérifie, mais un élément de rémunération réalisé auprès d'un autre employeur, qui peut ne pas être une collectivité publique. Toutefois, en raison du fait que l'agent public a l'obligation de communiquer ses activités accessoires et cas échéant une obligation de rétrocéder le revenu qui s'y rapporte, l'information relative à cette rémunération est susceptible de se retrouver entre les mains de la Confédération. La question se pose alors de savoir à quelles règles la communication de ce salaire doit obéir.

Les employés de la Confédération ne peuvent exercer pour un tiers une activité rémunérée que dans la mesure où ils ne violent pas leur devoir de fidélité (art. 20 al. 2 LPers). L'OPers prévoit un régime d'annonce, respectivement d'autorisation pour ces activités, selon qu'elles sont source de surcharge ou de conflit d'intérêts (art. 91 OPers ; ég. art. 23 LPers). L'art. 92 al. 1 OPers prévoit une obligation de remettre le revenu à la Confédération lorsque l'activité procède du contrat de travail avec la Confédération si la somme du revenu pour cette activité et le salaire excèdent 110% du montant maximal de la classe de salaire.

Les principes applicables à la communication des activités accessoires sont identiques à ceux guidant la pesée des intérêts pour la communication du salaire versé par la

143 TAF A-3609/2010 du 17 février 2011, c. 4.2.
144 TAF A-3609/2010 du 17 février 2011, c. 5.5.
145 Voir *supra* 1.
146 Sur la problématique de la transparence en matière d'activités accessoires, voir FLÜCKIGER et HÄNNI.

Confédération[147]. En particulier, il n'est pas fait de distinction quant au fait que la rémunération ne provient pas de deniers publics[148].

Le Tribunal administratif fédéral a ainsi admis, au nom de l'intérêt public à pouvoir vérifier que les règles en matière d'activités accessoires sont correctement appliquées, que les noms des cadres poursuivant des activités accessoires soient communiqués, ainsi que l'activité annexe exercée. En revanche, l'anonymat a été préservé pour les employés subalternes[149].

b) Fonction publique cantonale (CPDT-JUNE)

Le droit cantonal de la fonction publique ne contient pas de disposition relative à la protection des données des employés et fonctionnaires cantonaux. Le siège de la matière se trouve dans la CPDT-JUNE, qui vise à protéger la personnalité et les droits fondamentaux des personnes qui font l'objet d'un traitement de données personnelles, d'une part, et qui a pour but, notamment, de veiller à la transparence des activités et des autorités, d'autre part (art. 1 al. 2 et 3 CPDT-JUNE). Contrairement au droit fédéral, la réglementation relative à la protection des données et à la transparence figure dans un même texte, ce qui permet d'éviter des conflits liés au champ d'application de la matière et assure, probablement, une meilleure coordination matérielle lorsqu'une demande d'accès fondée sur le principe de transparence est de nature à porter atteinte à la sphère privée d'une personne.

La CPDT-JUNE s'applique aux autorités législatives, exécutives, administratives et judiciaires cantonales et aux organes qui en dépendent, aux communes et aux organes qui en dépendent, aux collectivités et établissements de droit public cantonaux et communaux, aux personnes de droit privé qui accomplissent des tâches d'intérêt public ou déléguées par une entité soumise à la loi et aux entités dans lesquelles une ou plusieurs entités soumises à la loi disposent ensemble d'une participation majoritaire, dans la mesure où elles accomplissement des tâches d'intérêt public (art. 2 CPDT-JUNE). Comme déjà relevé[150], le champ d'application de la CPDT-JUNE est plus large que celui de la LTrans, qui est limité, s'agissant des entités privées, à celles habilitées à rendre des décisions.

Pour ce qui est de la protection des données, la CPDT-JUNE se calque sur les définitions du droit fédéral[151] de même qu'elle en reprend, en substance, les conditions du traitement :

---

147 Voir *supra* ee).

148 TAF A_6738/2014 du 23 septembre 2015.

149 TAF A_6738/2014 du 23 septembre 2015, c. 5.2.3.2.

150 Voir *supra* A. 4.

151 Rapport LCPD, p. 11. Le canton de Neuchâtel s'était doté d'une loi sur la protection des données et d'une loi sur la transparence avant d'adopter la CPDT-JUNE ; celle-ci reprend les dispositions matérielles figurant dans celles-là : Rapport CDPT-JUNE, p. 30.

légalité, proportionnalité, bonne foi et finalité, exactitude et sécurité (art. 16 à 20 CPDT-JUNE). S'agissant de la communication des données à des tiers, elle ne peut intervenir que s'il existe une base légale, si la personne y a consenti en l'espèce ou a rendu ses données accessibles et ne s'est pas opposée à la communication, si elle s'y oppose dans le but d'empêcher le destinataire de faire valoir des prétentions juridiques ou si les données sont contenues dans un document demandé au titre de la transparence et que la communication est justifiée par un intérêt public prépondérant (art. 25 al. 1 CPDT-JUNE), conditions également analogues à ce qui prévaut en droit fédéral[152]. La communication des données est en outre refusée ou restreinte lorsqu'un intérêt public ou prépondérant l'exige (art. 26 al. 1 let. a CPDT-JUNE).

Pour ce qui est des demandes foncées sur le principe de transparence, la CPDT-JUNE prévoit qu'un intérêt privé prépondérant s'opposant à la transmission est reconnu lorsque le document officiel contient des données personnelles et que sa communication n'est pas autorisée par les règles applicables en matière de protection des données, à moins que la communication ne soit justifiée par un intérêt public prépondérant (art. 72 al. 3 let. a CPDT-JUNE).

Aussi, en droit cantonal, protection des données et transparence sont placées à pied d'égalité et l'arbitrage intervient à la lumière d'un intérêt public prépondérant, cette notion ayant une portée identique à l'art. 25 et à l'art. 72 CDPT-JUNE[153]. Les situations dans lesquelles un intérêt public peut être prépondérant sont énumérées à l'art. 72 al. 2 CPDT-JUNE. Parmi ceux-ci figure l'intérêt public à ne pas affaiblir la position de négociation d'une autorité (art. 72 al. 2 let. d CPDT-JUNE), point qui sera abordé *infra* V.B.2.

La jurisprudence cantonale est peu fournie, mais il en ressort qu'elle se calque dans une très grande mesure sur les critères et solutions retenus en droit fédéral[154]. Ce qui a été dit plus haut s'agissant de la communication du salaire et des activités accessoires des agents publics devrait donc valoir dans la même mesure pour la fonction publique cantonale.

IV. À quelles conditions un travailleur peut-il communiquer son salaire à un tiers ?

Nous avons vu dans le chapitre précédent que le salaire constitue un élément de la personnalité de l'employé que celui-ci peut en principe légitimement considérer comme une donnée confidentielle, sauf si l'employeur se prévaut d'un motif justificatif pour le

[152] Rapport CPDT-JUNE, p. 33.
[153] Rapport LCPD, p. 26.
[154] CDP.2014.23 du 28 janvier 2016.

communiquer à un tiers. Il est toutefois possible de traiter la question de la confidentialité du salaire sous un angle diamétralement différent. En effet, l'employeur peut avoir intérêt à ce que le montant des salaires versés reste confidentiel ne serait-ce que pour éviter des revendications salariales ou le débauchage de ses employés. À l'inverse, l'employé peut souhaiter communiquer le montant de son salaire à des tiers, à l'intérieur ou l'extérieur de l'entreprise. Il s'agit dans ce chapitre de déterminer à quelles conditions une telle communication s'avère licite. À notre avis, il n'existe pas de solution schématique, car il convient de procéder dans chaque cas d'espèce à une pesée des intérêts. Les intérêts entrant en jeu ne sont pas les mêmes qu'il s'agisse du droit privé du travail ou du droit de la fonction publique, car toute limitation du droit de l'agent public de s'exprimer est examinée sous l'angle de la violation de ses droits fondamentaux, notamment la liberté d'expression. Cela impose une plus grande retenue à l'employeur.

A. En droit privé du travail

Après avoir rappelé les intérêts en présence (**1.**), nous déterminerons comment doit s'effectuer la pesée des intérêts dans quelques cas d'application (**2.**). Nous examinerons également la portée d'une clause de confidentialité (**3.**).

1. Intérêts en présence

Pour déterminer à quelles conditions, un employé a le droit de communiquer le montant de son salaire à un tiers, il faut tenir compte des intérêts en présence, potentiellement contradictoires, de l'employé (**a**) et de l'employeur (**b**).

a) Liberté de l'employé

Le droit pour chaque employé de communiquer son salaire à un tiers peut être déduit des règles sur la protection de la personnalité (art. 328 CO) qui lui confère une certaine liberté en la matière, d'un double point de vue. Tout d'abord, l'employeur doit tolérer, dans certaines limites, l'exercice des libertés individuelles dans l'entreprise[155]. Chaque employé dispose ainsi d'un certain droit à la liberté d'expression qui lui permet de s'exprimer même publiquement sur la vie de l'entreprise et de formuler, de bonne foi, des critiques et des propositions[156].

Par ailleurs, l'employé peut en principe librement fixer les éléments entrant dans sa sphère privée. Il est ainsi libre de partager les événements de sa vie à un cercle de personnes

[155] DUNAND, N 16 *ad* art. 328 CO, p. 275.
[156] BRUNNER/BÜHLER/WAEBER/BRUCHEZ, N 10 *ad* art. 328 CO, p. 146.

déterminées ou de les divulguer publiquement, délimitant ainsi concrètement ce qui relève de sa sphère intime, privée et publique.

b) Protection de l'employeur

L'employeur peut également se prévaloir des droits de la personnalité, même lorsqu'il est une entité ayant la personnalité morale. En effet, les articles 28 ss CC protègent la personnalité sociale d'une personne morale, qui comprend le droit à l'honneur, la sphère privée et la personnalité économique[157]. Mais la règle de protection la plus pertinente dans notre contexte réside dans l'article 321a al. 1 CO, selon lequel le travailleur doit exécuter avec soin le travail qui lui est confié et sauvegarder fidèlement les intérêts légitimes de l'employeur. Nous distinguerons le principe général et la protection du secret d'affaires.

aa) Devoir de diligence et de fidélité

L'obligation de fidélité consiste à mettre toutes ses forces au service de son employeur et à renoncer à tout ce qui pourrait lui nuire : elle comporte ainsi un aspect positif et un aspect négatif[158]. Positivement, le travailleur doit se consacrer entièrement à l'exécution de sa tâche et avertir l'employeur d'éventuels dommages imminents, des perturbations dans l'exécution du travail et d'autres irrégularités ou abus[159]. Négativement, le travailleur doit s'abstenir de tout comportement susceptible de léser son employeur dans ses intérêts légitimes et éviter, en particulier, tout ce qui pourrait lui causer un dommage économique[160].

L'étendue et la mesure de l'obligation de diligence et de fidélité doivent être analysées en fonction de la position du travailleur dans l'entreprise. En raison du crédit particulier et de la responsabilité que lui confère sa fonction dans l'entreprise, le comportement d'un cadre sera apprécié avec une rigueur accrue[161]. Étant en principe liée aux rapports de travail, l'obligation de fidélité ne s'étend généralement pas à la vie privée et sociale du travailleur[162].

bb) Protection des secrets d'affaires

Selon l'art. 321a al. 4 CO, qui précise la notion du devoir de diligence et de fidélité, le travailleur ne doit pas utiliser ni révéler des faits destinés à rester confidentiels, tels que

---

157 JEANDIN, N 20 *ad* art. 28 CC, p. 249.
158 DUNAND, N 12 *ad* art. 321a CO, p. 56.
159 TF 4A_297/2016 du 17 novembre 2016, c. 4.3.1.
160 TF 4A_297/2016 du 17 novembre 2016, c. 4.2.
161 ATF 127 III 86, c. 2c.
162 BRUNNER/BÜHLER/WAEBER/BRUCHEZ, N 4 *ad* art. 321a CO, p. 56.

les secrets de fabrication et d'affaires dont il a pris connaissance au service de l'employeur. Pendant la durée du contrat, cette obligation est absolue, alors qu'elle ne perdure après la fin des rapports contractuels que dans les limites de la sauvegarde des intérêts légitimes de l'employeur[163].

Constitue un secret, au sens de cette disposition, toute connaissance particulière qui n'est pas de notoriété publique et qui n'est pas facilement accessible, dont un commerçant ou un fabricant à un intérêt légitime à conserver l'exclusivité et qu'il n'entend pas divulguer[164]. Il faut et suffit que le travailleur ait pris connaissance de ces faits alors qu'il était au service de son employeur, peu importe la manière[165]. Les secrets de fabrication comprennent les procédés de production et de fabrication à caractère technique, ainsi que les plans de construction[166]. Quant aux secrets d'affaires, ils comprennent la pratique et l'organisation commerciale et financière de l'entreprise (notamment : liste de clients, calculs des prix, marges de bénéfice, marketing)[167]. Ils peuvent aussi consister en des données personnelles concernant l'employeur ou des collègues de travail[168]. Pour être qualifiées de secrets de fabrication ou d'affaires, les connaissances acquises par le travailleur doivent toucher à des questions techniques, organisationnelles ou financières qui sont spécifiques : il ne peut s'agir de connaissances pouvant être acquises dans toutes les entreprises de la même branche[169].

D'une manière générale, le devoir de discrétion de l'employé ne s'étend pas aux conditions de travail dans l'entreprise[170], ni au salaire versé[171]. Le salaire de chaque travailleur ne constitue en effet pas une connaissance acquise à l'occasion du rapport de travail, mais un élément essentiel du contrat de travail qui a fait l'objet d'une clause contractuelle. Une autre question est de déterminer quel est le statut d'informations globales concernant la structure et le montant des salaires dans une entreprise. Il nous semble que des données précises sur la masse salariale d'une entreprise sont susceptibles de constituer un secret d'affaires puisqu'elles permettent d'en déterminer l'un des éléments principaux de l'organisation commerciale et financière. Il en va de même d'une liste de salariés de l'entreprise avec indication de leurs salaires. Dans une affaire concernant la branche des taxis, le Tribunal fédéral a cependant considéré que l'employeur n'était pas parvenu à

163 TERCIER/BIERI/CARRON, N 2816.
164 Arrêt du Tribunal cantonal du canton de Vaud du 27 avril 2007, c. II.c, *in* : JAR 2008, p. 497.
165 STREIFF/VON KAENEL/RUDOLPH, N 12 *ad* art. 321a CO, p. 194 ; SUBILIA/DUC, N 24 *ad* art. 321a CO, p. 125.
166 SUBILIA/DUC, N 25 *ad* art. 321a CO, p. 126.
167 SUBILIA/DUC, N 25 *ad* art. 321a CO, p. 126.
168 REHBINDER/STÖCKLI, N 13 *ad* art. 321a CO, pp. 137-138.
169 ATF 138 III 67, c. 2.3.2.
170 Arrêt du Tribunal d'appel du canton du Tessin du 1er février 2013, c. 5, *in* : JAR 2014, p. 493.
171 CRAMER, p. 1482.

démontrer, dans les circonstances du cas d'espèce, en quoi la connaissance des salaires versés dans l'entreprise pouvait constituer un secret d'affaires[172].

2. Pesée des intérêts

Il peut sembler qu'il existe une contradiction irréconciliable entre la liberté dont peut se prévaloir l'employé et le devoir de fidélité auquel il est soumis. Cette contradiction n'est toutefois qu'apparente, car autant les droits de la personnalité que le devoir de fidélité sont limités. En effet, dans l'exercice de ses droits de la personnalité, l'employé doit tenir compte des intérêts légitimes de son employeur qui sont notamment fondés sur les exigences du travail à effectuer[173]. Par ailleurs, le devoir de fidélité est lui-même limité par les droits de la personnalité de l'employé[174]. Pour trouver une solution harmonieuse, il y a donc lieu d'effectuer dans chaque cas d'espèce une pesée des intérêts en présence entre l'intérêt de l'employé à la communication et celui de l'employeur au maintien d'une certaine confidentialité.

Nous traiterons ici de trois cas d'application, à savoir la communication du salaire à des collègues de travail (**a**), la critique de la politique salariale de l'entreprise (**b**) et la communication du salaire à des concurrents de l'employeur (**c**).

a) Communication du salaire à des collègues de travail

Le devoir de diligence et de fidélité n'impose pas à l'employé une obligation générale de s'abstenir de communiquer son salaire à autrui, et en particulier à ses collègues de travail[175]. Au contraire, le droit de rendre public le montant de sa rémunération fait, en principe, partie des droits de la personnalité des travailleurs[176].

Le Tribunal fédéral a eu l'occasion de préciser qu'un employé a parfaitement le droit de parler à des collègues moins bien rémunérés que lui de son propre salaire et de les encourager à demander des augmentations à l'employeur. Son licenciement immédiat pour cette raison s'avère donc injustifié. Et notre Haute Cour de préciser que chaque travailleur peut de toute manière solliciter en tout temps une amélioration de ses conditions de travail, que l'employeur acceptera ou non, dans le cadre de négociations et du jeu de l'offre et la demande[177]. L'intérêt de l'employé à la communication est donc prépondérant.

---

172 TF 4A_283/2010 du 11 août 2010, c. 2.7.

173 DUNAND, N 12 *ad* art. 328 CO, p. 274 ; STREIFF/VON KAENEL/RUDOLPH, N 5 *ad* art. 321a CO, pp. 177-178.

174 PORTMANN/RUDOLPH, N 17 *ad* art. 321a CO, p. 1843 ; TERCIER/BIERI/CARRON, N 2809.

175 CRAMER, p. 1482 ; STREIFF/VON KAENEL/RUDOLPH, N 12 *ad* art. 321a CO, p. 195.

176 BRUNNER/BÜHLER/WAEBER/BRUCHEZ, N 12 *ad* art. 328 CO, p. 147.

177 TF du 14 décembre 1994, *in* : JAR 1995 214. Voir aussi TF 4A_283/2010 du 11 août 2010, c. 2.

On peut toutefois imaginer d'autres situations dans lesquelles la communication de salaires à des collègues sera constitutive d'une violation du devoir de fidélité. Tel sera le cas, par exemple, lorsqu'un cadre informe ses subordonnés du montant du salaire de certains employés de l'entreprise dont il a eu connaissance à l'occasion de son travail. En effet, en communiquant les salaires dans un tel contexte, le cadre violera son devoir de fidélité dans la mesure notamment où la diffusion de ces informations représentera une atteinte potentielle à la personnalité des employés concernés, dont l'employeur devra répondre (art. 55 CC ; art. 55 et 101 CO)[178]. L'intérêt de l'employeur à la non-communication pourra s'avérer prépondérant. Notons toutefois que le Tribunal d'appel du canton du Tessin a considéré que, dans les circonstances du cas d'espèce, le licenciement immédiat d'un cadre qui avait communiqué à une subordonnée le montant des salaires perçus par d'autres collaborateurs était injustifié[179].

b) Critique de la politique salariale de l'entreprise

Un employé peut-il critiquer librement la politique salariale de l'entreprise ? Selon le Tribunal fédéral, un employé a la possibilité de formuler certaines critiques envers son employeur, même publiquement, car il exerce sa liberté d'opinion, pour autant qu'il le fasse de manière objective, sans tomber dans la polémique[180]. Le devoir de fidélité du travailleur et les rapports de confiance qui sont à la base du contrat de travail peuvent cependant tempérer le droit de critiquer et même justifier, dans certaines circonstances, le licenciement du travailleur[181]. Ainsi, un cadre n'a pas à communiquer à ses subordonnés des informations relatives à des dissensions importantes qui l'opposent à la direction de l'entreprise[182]. Il faut donc peser les intérêts en présence dans chaque cas d'espèce. On peut considérer qu'un employé qui critiquerait publiquement et sans raison objective le système de rémunération existant dans l'entreprise violerait son devoir de fidélité[183]. En effet, dans un tel cas le travailleur ne pourrait se prévaloir d'aucun intérêt digne de protection.

En revanche, une critique publique de la politique salariale de l'entreprise pourra notamment s'opérer de manière licite dans le cas où l'employeur viole de manière répétée ses obligations légales et conventionnelles en la matière. Ce droit d'expression sera nécessaire à l'activité syndicale[184].

---

178 CRAMER, p. 1482.
179 Arrêt du 1er février 2013, c. 5, *in* : JAR 2014, p. 493.
180 TF 4C.91/2002 du 23 novembre 2001, c. 3a.
181 TF 4C.129/2003 du 5 septembre 2003, c. 4.2.
182 TF 4C.400/2004 du 14 février 2005, c. 3.
183 CRAMER, p. 1482.
184 BRUNNER/BÜHLER/WAEBER/BRUCHEZ, N 12 *ad* art. 328 CO, p. 147.

c) Communication du salaire à un concurrent

Le salaire de chaque travailleur ne constitue pas un secret d'affaires ni une information dont la divulgation impliquerait une violation du devoir de fidélité. Un travailleur est donc en principe libre de communiquer son propre salaire à l'extérieur de l'entreprise. Il a notamment la possibilité d'indiquer le montant de son salaire à un concurrent de son propre employeur, notamment dans le cadre de négociations précontractuelles en vue de la conclusion d'un contrat de travail. D'une manière générale, on reconnaît au travailleur le droit, déduit de son intérêt légitime au libre épanouissement de sa personnalité, de préparer une activité future, pour autant qu'il respecte les règles de la bonne foi et qu'il ne contrevienne pas à une éventuelle clause d'interdiction de concurrence[185]. Il n'est en principe pas tenu d'en informer son employeur[186]. Dans un arrêt déjà cité ci-dessus, le Tribunal fédéral a d'ailleurs indiqué que l'on ne voit pas ce qui empêcherait des collaborateurs abordés par des employeurs potentiels de divulguer leurs propres revenus[187]. Leurs intérêts à la communication sont prépondérants.

D'autres situations impliqueront en revanche une violation du devoir de fidélité. L'employé doit s'abstenir de diffuser à des tiers des documents internes[188] ou de confier à des tiers des faits que l'employeur a qualifiés de secrets ou dont le caractère confidentiel ressort des circonstances[189]. Par ailleurs, des secrets appréhendés de manière irrégulière doivent dans tous les cas s'en voir interdire l'exploitation[190]. Une liste comportant les salaires des employés de l'entreprise nous paraît remplir ces conditions. Nous considérons que la structure des salaires et la masse salariale d'une entreprise constituent des secrets d'affaires qu'un employé ne saurait communiquer à un concurrent de l'employeur sans violer gravement son devoir de fidélité.

3. Clause de confidentialité

Selon l'article 321d alinéa 1 CO, l'employeur peut établir des directives générales sur l'exécution du travail et la conduite des travailleurs et leur donner des instructions particulières. Ces directives, qui tendent à préciser le devoir de diligence et de fidélité du travailleur, portent sur les besoins de l'entreprise (objet du travail, temps, lieu et organisation), sur la manière d'accomplir la prestation et sur le comportement des travailleurs[191]. Elles trouvent leur limite dans le respect des règles de la bonne foi

185 ATF 138 III 67, c. 2.3.5 ; ATF 117 II 72, c. 4a-b, *in* : JdT 1992 I 569.
186 TF du 13 septembre 1994, c. 2a, *in* : JAR 1995, p. 203.
187 TF 4A_195/2010 du 8 juin 2010, c. 2.3. Dans le même sens, TF 4A_283/2010 du 11 août 2010, c. 2.
188 AUBERT, Commentaire, N 7 *ad* art. 321a CO, p. 1977.
189 AUBERT, Commentaire, N 7 *ad* art. 321a CO, p. 1977 ; WYLER/HEINZER, p. 82.
190 SCHLOSSER, p. 75.
191 PORTMANN/RUDOLPH, N 3 *ad* art. 321d CO, p. 1856.

(cf. art. 321d al. 2 CO) et des droits de la personnalité des travailleurs[192]. Nous ne pensons pas que l'employeur puisse imposer par voie de directives un devoir de discrétion relatif au salaire. Un tel procédé serait autant étranger à la nature du droit de donner des directives que contraire aux droits de la personnalité des travailleurs concernés.

Une autre question est de savoir si les parties au contrat de travail peuvent valablement convenir d'une clause de confidentialité prohibant, sous peine de sanction, toute communication du montant du salaire à des tiers. La question est controversée. On rappellera qu'un accord de confidentialité ou de discrétion a pour objet de définir les conditions dans lesquelles une information sera gardée secrète[193]. En pratique une telle clause peut être convenue au moment de la conclusion du contrat de travail ou ultérieurement. Elle sera souvent assortie d'une clause pénale prévoyant le paiement d'une peine conventionnelle en cas de non-respect (cf. art. 163 CO).

Selon des auteurs, les « clauses contractuelles ou réglementaires indiquant que le salaire est confidentiel, de même que les injonctions orales qui recommandent de ne pas révéler le montant du salaire individuel sont illicites et nulles. Elles constituent une limitation des droits de la personnalité des travailleurs qui n'est justifiée par aucun intérêt prépondérant de l'employeur (art. 28 al. 2 CC). En effet, elles n'ont pour finalité que d'empêcher les travailleurs d'effectuer des comparaisons et de formuler des revendications »[194].

Selon un autre auteur, au contraire, de telles clauses de confidentialité sont en principe parfaitement valables : « Mitunter finden sich in Arbeitsverträgen Bestimmungen, die den Arbeitnehmer verpflichten, "über die Höhe der Vergütung absolutes Stillschweigen" zu bewahren. Solche Geheimhaltungsabreden zu Lasten des Arbeitnehmers sind grundsätzlich zulässig. Sie stellen keine Persönlichkeitsverletzung dar, da sie den Arbeitnehmer in keiner Form übermässig binden oder seine Würde tangieren »[195].

L'article 321a CO est de droit dispositif. L'obligation de diligence et de fidélité peut ainsi être étendue ou limitée par une convention entre les parties[196]. Lorsqu'elles la définissent de manière plus stricte que ne le prévoit cette disposition légale, l'accord dérogatoire doit cependant respecter les limites de la liberté contractuelle, notamment de l'article 27 alinéa 2 CC[197]. Plus généralement, l'obligation de fidélité trouve ses limites dans les intérêts légitimes du travailleur, protégés par l'article 328 CO, qui comprennent le droit au

192 TF 2C_103/2008 du 30 juin 2008, c. 6.2.
193 Cf. DESSEMONTET, p. 28.
194 BRUNNER/BÜHLER/WAEBER/BRUCHEZ, N 12 *ad* art. 328 CO, p. 147.
195 CRAMER, p. 1482.
196 ATF 117 II 72, c. 4a, *in* : JdT 1992 I 569.
197 TF 4A_408/2011 du 15 novembre 2011, c. 5.4.1.

libre épanouissement de sa personnalité et le droit à la sauvegarde de ses intérêts financiers[198].

Quant à l'article 328 CO, étant de nature relativement impérative, les parties ne peuvent lui déroger qu'en faveur du travailleur (art. 362 CO). La difficulté en l'espèce résulte du fait que, comme nous l'avons vu, l'art. 328 CO protège autant la confidentialité du salaire que sa libre communication par le travailleur. Ainsi, si une clause de confidentialité est généralement dans l'intérêt de l'employeur, on ne peut exclure qu'elle soit aussi convenue, du moins partiellement, dans l'intérêt du travailleur, par exemple lorsqu'il ne souhaite pas que le montant de son salaire qui vient d'être majoré soit divulgué à ses collègues. Selon ce qui précède, une clause de confidentialité nous paraît pouvoir être valable dans les limites des règles générales (art. 27 al. 2 CC ; art. 328 et 341 CO).

La portée de ce type de clause de confidentialité sera toutefois doublement limitée dans le cadre d'une procédure judiciaire. Tout d'abord, il va de soi qu'elle ne saurait priver l'employé d'agir en justice pour faire valoir ses propres prétentions salariales. Ensuite, elle ne sera généralement pas opposable au collègue de travail qui fait lui-même valoir de telles prétentions, et qui, comme nous l'avons vu, pourra généralement solliciter avec succès la production par l'employeur des données salariales du travailleur concerné.

B. En droit de la fonction publique

L'agent public, comme tout citoyen, dispose du droit à l'autodétermination informationnelle (art. 13 al. 2 Cst.) ainsi que du droit à la libre expression (art. 16 Cst.)[199], qui doivent lui permettre de s'exprimer librement et de communiquer à des tiers ou au public des informations qui le concernent. Toutefois, en raison du rapport de droit spécial qui le lie à l'État, des restrictions particulières à ces libertés sont tolérées, fondées sur son devoir général de fidélité à l'égard de l'État, qui est son employeur (**1.**). Mais à notre sens cela n'est pas propre à l'empêcher de communiquer le montant de son salaire à des tiers (**2.**) ou selon les circonstances de critiquer la politique salariale de l'État (**3.**).

1. Le devoir de fidélité

En droit fédéral, le devoir général de diligence et de fidélité des employés de la Confédération est réglé à l'art. 20 al. 1 LPers. En vertu de cette disposition, l'employé est tenu d'exécuter avec soin le travail qui lui est confié et de défendre les intérêts légitimes de la Confédération et de son employeur.

198 TF 4C.442/1996 du 30 avril 1997, c. 3b, *in* : sic ! 1997, p. 382.
199 ATF 141 I 201, c. 4.1.

Le devoir de fidélité et de sauvegarde des intérêts se rapporte en première ligne à l'obligation principale de l'employé, à savoir aux prestations de travail qu'il doit fournir. Ainsi, l'employé a l'obligation d'accomplir son travail fidèlement et consciencieusement, mais également d'éviter et d'annoncer les risques ou de veiller sur les affaires confiées. L'étendue du devoir de fidélité qui lui incombe s'inspire de l'art. 321a CO. Mais à la différence de l'art. 321a al. 1 CO, le devoir de fidélité issu de la LPers contient une « double obligation de loyauté » dans la mesure où l'employé soumis à la LPers ne se doit pas uniquement de sauvegarder les intérêts publics et d'être loyal envers son employeur (devoir de confiance particulier), mais également – en tant que citoyen – envers l'État (devoir de confiance général). Le devoir de fidélité vise à assurer le fonctionnement de l'administration publique, de façon à ce que la confiance des administrés placée dans l'État ne soit pas décrédibilisée. L'étendue du devoir de fidélité dépend fortement de la place de l'employé dans le service ; si l'employé est un cadre, ledit devoir sera plus élevé que s'il s'agit d'un subordonné[200].

Du devoir de fidélité découle le secret de fonction (art. 22 LPers). Le secret de fonction couvre tous les faits et informations que l'agent apprend dans l'exercice de ses fonctions. Ces faits doivent être secrets en ce sens qu'ils ne sont connus que d'un cercle restreint de personnes et que le maître du secret veut les garder confidentiels, pour autant qu'il y ait un intérêt[201].

En droit cantonal, le devoir de fidélité et le secret de fonction sont consacrés aux art. 15 et 20 LSt. Leur portée est identique à celle valant en droit fédéral.

2. La communication du salaire à des tiers

La communication de son salaire par l'agent public relève du droit à l'autodétermination informationnelle et de la liberté d'expression, tous deux garantis par la Constitution. Une interdiction de communiquer son salaire par l'agent public constituerait à notre sens une atteinte grave à ses droits fondamentaux. En effet, dans le même sens, le Tribunal fédéral a considéré que l'interdiction faite au destinataire d'une décision constitue une atteinte grave à son droit à l'autodétermination en matière d'informations et à sa liberté d'expression[202].

Pour qu'une telle restriction soit admissible, la collectivité publique doit disposer d'une base légale[203]. Or, il n'existe pas en droit fédéral ou cantonal de la fonction publique de norme posant ce type de restriction à l'agent public. À notre sens, le devoir général de

200 TAF A-5420/2015 du 11 décembre 2015, c. 3.3.2.

201 ATF 141 IV 65, c. 4.

202 ATF 141 I 201, c. 4.

203 *Ibid*. Compte tenu du rapport de droit spécial liant l'agent public à l'Etat, une base légale matérielle pourrait être admise.

fidélité ne suffit pas à lui seul à consacrer une telle interdiction puisqu'on voit mal dans quelle mesure la communication de son salaire par un agent public puisse être de nature à entraver le bon fonctionnement de l'administration et à décrédibiliser la confiance des citoyens en l'État.

En outre, le montant du salaire d'un agent public n'est pas une information qui relève du secret de fonction à notre avis. Il ne s'agit à notre sens pas d'une information que l'agent public a apprise dans le cadre de son travail, mais d'une information inhérente à sa qualité d'employé. Au demeurant, s'agissant de son propre salaire, il doit être considéré comme le maître du secret s'y rapportant.

Enfin, la législation en matière de protection des données a pour objet de protéger la sphère privée des particuliers, non de les limiter dans la communication des données qui les concernent ; les art. 12 al. 3, 19 al. 1 let. c LPD et 25 al. 1 let. b CPDT-JUNE autorisent en effet la communication des données que la personne a rendues accessibles.

Aussi, faute de base légale interdisant à l'agent public de communiquer le montant de son salaire, celui-ci conserve la possibilité de faire connaître à des tiers le montant de sa rémunération.

3. La critique de la politique salariale de l'État

Critiquer la politique salariale de l'État relève également de la liberté d'expression. Comme déjà indiqué, il est admis que la liberté d'expression des agents publics puisse être restreinte par le devoir de fidélité qui leur incombe, lequel s'étend aussi au comportement en dehors du service[204].

De manière générale, la critique de l'activité de l'État n'est pas exclue, mais l'employé public, en raison de sa position, doit s'imposer une certaine retenue dans la manière dont il la formule. Il lui revient d'épuiser d'abord les voies internes pour contester la situation qu'il critique et il ne peut s'adresser au public que s'il n'y a pas d'autres moyens efficaces[205]. Si l'employé de l'État dispose d'une relative liberté pour aborder publiquement des sujets de société, il doit observer un devoir de réserve (et de discrétion) lorsqu'il s'exprime dans le domaine de ses activités ou sur les affaires de son service, ce d'autant plus lorsque les propos tenus visent des personnes identifiables[206]. Lorsqu'il s'agit d'apprécier dans une situation concrète dans quelle mesure les propos tenus s'inscrivent dans le cadre de la liberté d'opinion et d'expression, il y a lieu de retenir différents critères: le rang hiérarchique de la personne qui diffuse le message ; la nature et le contenu du

[204] ATF 136 I 332, c. 3.2.
[205] ATF 136 I 332, c. 3.2.2.
[206] TAF A-6723/2013 du 28 janvier 2015, c. 8.1.4.

message ; le lieu et le moment de diffusion du message, dans ou hors du service ; les destinataires du message, selon qu'il est diffusé dans un cadre professionnel ou privé ; et la manière dont le message a été formulé et transmis[207].

S'agissant de la critique de la politique salariale de l'État par les agents publics, celle-ci est admise très largement dans la mesure où elle relève de la prise de position par rapport à des mesures d'économie ayant une portée générale et relevant du budget voté par le détenteur du pouvoir législatif. Selon les cas, cette critique peut s'exprimer en allant jusqu'à la grève[208], accompagnée de manifestations sur la voie publique. Les agents disposant d'une position hiérarchique élevée doivent à notre sens faire preuve de retenue compte tenu du devoir de fidélité accru qui est le leur, laquelle doit s'exercer notamment vis-à-vis des personnes qui leur sont subordonnées ; mais cela ne signifie pas encore qu'ils ne puissent pas user d'autres moyens, notamment judiciaires, pour exprimer leur mécontentement[209].

V. Quelle est la valeur d'une clause de confidentialité contenue dans une convention de départ ?

Dans le cadre d'un accord de résiliation ou convention de départ, les parties définissent les modalités de la fin des rapports de travail, en particulier la date de la fin du contrat, ainsi que les conditions financières. Elles y intègrent souvent des indemnités de départ qui peuvent prendre diverses formes[210], ainsi qu'une clause de confidentialité selon laquelle elles s'engagent, peine conventionnelle à l'appui, à ne pas révéler le contenu de la transaction. La question de la valeur juridique d'une telle clause nous semble pertinente dans le cadre de notre contribution puisque les indemnités prévues peuvent être de nature salariale. Au demeurant, la thématique des conventions de départ a fait l'objet de décisions de justice s'agissant de départs d'agents publics ou d'employés d'entités privées soumises à la législation sur la transparence.

---

207 TAF A-6723/2013 du 28 janvier 2015, c. 8.1.5 ; MATTHEY, p. 364.

208 SJ 1995 p. 681.

209 Voir le recours formé par l'Union des cadres de l'administration cantonale genevoise contre une loi modifiant leur traitement : ACST/13/2015 du 30 juillet 2015 (Chambre constitutionnelle de la Cour de justice, Genève).

210 Sur les indemnités de départ en droit du travail, cf. URBEN, pp. 160 ss.

A. En droit privé du travail

Après un rappel des modalités d'un accord de résiliation (**1.**), nous traiterons plus spécifiquement des effets d'une clause de confidentialité (**2.**).

1. Accord de résiliation

L'accord de résiliation permet aux parties de mettre fin à un contrat de travail de durée déterminée ou indéterminée sans respecter la date d'échéance normalement prévue (pour un contrat de durée déterminée) ou le délai de congé applicable (pour un contrat de durée indéterminée). Il est en effet admis que les parties peuvent rompre en tout temps le contrat de travail pour autant qu'elles ne cherchent pas à détourner ainsi une disposition impérative de la loi (art. 361 et 362 CO)[211]. Selon la jurisprudence, la validité d'un accord de résiliation est soumise au respect de deux conditions cumulatives. Il faut, d'une part, que l'accord ait été librement consenti (**a**), et d'autre part qu'il contienne des concessions réciproques d'importance comparable (**b**). Lorsqu'il constate que ces conditions ne sont pas réalisées, le juge applique les dispositions du régime légal ordinaire (**c**).

a) Accord librement consenti

L'accord de résiliation n'est soumis à aucune exigence de forme[212]. La jurisprudence précise toutefois qu'un accord par actes concluants ne saurait être admis qu'avec retenue. Il est ainsi nécessaire que la volonté commune des parties de se départir du contrat soit établie sans équivoque[213]. Lorsque l'accord de résiliation a été préparé par l'employeur ou un tiers mandaté par lui, un temps de réflexion suffisant doit être octroyé au travailleur[214]. Par ailleurs, il ne faut pas que l'employé se soit trouvé dans une position de faiblesse, par exemple en raison de fortes pressions liées à une restructuration ou un état de santé dégradé[215].

b) Accord contenant des concessions réciproques

Dans le cadre d'un accord de résiliation, l'employé consent à d'importantes concessions puisqu'il renonce en principe à la protection contre les congés, en particulier aux règles sur le congé abusif (art. 336 CO) ou sur la résiliation en temps inopportun (art. 336c CO). Il verra également ses droits envers l'assurance-chômage péjorés (cf. art 30 al. 1 let. a

---

211 BONARD, N 14 *ad* art. 335 CO, p. 582 ; STREIFF/VON KAENEL/RUDOLPH, N 10 *ad* art. 335 CO, p. 906.
212 TF 4A_474/2008 du 13 février 2009, c. 3.1.
213 TF 4A_563/2011 du 20 janvier 2012, c. 4.1.
214 Cf. BONARD, N 14 *ad* art. 335 CO, p. 582 et références citées.
215 TF 4A_376/2010 du 30 septembre 2010, c. 3. Voir aussi WYLER/HEINZER, p. 528.

LACI). L'employeur doit consentir à des concessions d'importance comparable[216]. Entrent notamment en considération, la libération de l'obligation de travailler et le droit simultané de reprendre un nouvel emploi sans imputation sur le salaire, le paiement du salaire pour un temps plus long que le délai de résiliation contractuel ou légal, le paiement d'une indemnité de départ ou encore l'octroi d'une aide à la reconversion[217].

L'étendue des concessions doit être appréciée au moment de la conclusion de l'accord, selon les chances de faire valoir avec succès les prétentions auxquelles il est renoncé[218]. Selon la jurisprudence, il convient toutefois de réserver les évènements imprévisibles pouvant survenir jusqu'à la fin du délai de congé, et imputables à aucune des parties, tels que la survenance d'une période de protection en raison d'une incapacité de travail[219].

c) Accord invalide

L'accord qui ne correspond pas à un accord librement consenti ou qui ne comporte pas de véritables concessions réciproques ne lie pas les parties[220]. Selon la jurisprudence, il convient alors de faire abstraction de cet accord invalide qui ne produit aucun effet et d'appliquer les dispositions relevant du régime légal ou conventionnel ordinaire[221].

Relevons toutefois qu'en principe, la réalisation des conditions de la libre formation de la volonté du travailleur et de la réciprocité suffisante des concessions devrait être présumée, lorsque le travailleur a été assisté par un avocat ou un autre mandataire professionnellement qualifié au moment de la négociation[222]. En effet, dans une telle circonstance, l'employé est censé avoir été renseigné sur l'étendue de ses droits et les conséquences de la conclusion d'un tel accord[223].

2. Clause de confidentialité

Les clauses de confidentialité qui complètent assez souvent les accords de résiliation ou les conventions de départ relèvent de la liberté contractuelle et doivent donc être en principe respectées. L'employé peut donc parfaitement s'engager à ne pas révéler à des tiers le contenu de l'accord, sous réserve évidemment du respect des règles impératives de

216 TF 4A_563/2011 du 19 janvier 2012, c. 4.1.
217 BONARD, N 15 *ad* art. 335 CO, p. 583.
218 WYLER/HEINZER, p. 528.
219 TF 4A_376/2010 du 30 septembre 2010, c. 3 ; TF 4C.27/2002 du 19 avril 2002, c. 2.
220 BONARD, N 16 *ad* art. 335 CO, p. 583.
221 TF 4A_495/2007 du 12 janvier 2009, c. 4.3.1.2.
222 WYLER/HEINZER, p. 530.
223 BOHNET/DIETSCHY, N 21 *ad* art. 341 CO, p. 874.

l'ordre juridique (obligations fiscales, obligations des dirigeants des sociétés cotées en bourse, etc.).

L'employé ne saurait toutefois se lier par une convention qui le priverait de la protection des dispositions impératives (art. 341 CO) ou qui constituerait un engagement excessif (art. 27 al. 2 CC). En cas de contestation de la validité ou du contenu de l'accord, l'employé a toujours la possibilité de soumettre la convention à un juge. Celui-ci pourra notamment s'assurer que l'employé n'a pas renoncé sans compensation suffisante à des droits résultant de dispositions impératives, faute de quoi l'art. 341 al 1 CO serait vidé de sa substance[224]. Autrement dit, une clause de confidentialité n'interdit pas à l'employé d'actionner son employeur en justice pour faire valoir des créances protégées par des dispositions impératives.

B. En droit de la fonction publique

Il sort du champ de la présente contribution d'étudier l'admissibilité de conventions de départ entre une collectivité publique et l'un de ses agents, respectivement de leur contenu. Quelques éléments seront néanmoins précisés (**1.**) puisqu'il n'est pas rare que cet instrument soit utilisé en pratique. Nous examinerons ensuite la convention de départ à l'épreuve du principe de transparence (**2.**).

1. Les conventions de départ en droit de la fonction publique

En cas de litige entre une collectivité publique et un de ses agents, la fin de la relation de travail peut être imposée par la collectivité, qui prononce un licenciement ou la révocation de l'agent par la voie de la décision. Le départ peut toutefois aussi être convenu d'entente entre les parties, permettant selon les cas d'éviter une procédure pouvant être longue et coûteuse.

La voie contractuelle est prévue dans le régime de la LPers pour mettre fin aux rapports de travail (art. 13 et 34 al. 1 et LPers). Il s'agit même de la voie qui doit être préférée à la décision unilatérale compte tenu de la contractualisation de mise dans ce domaine[225]. Pour ce qui est de l'indemnité pouvant être versée, il s'agit de se référer à l'art. 19 al. 4 LPers, qui renvoie aux dispositions d'exécution, en l'occurrence les art. 78 et 79 OPers. Pour prétendre à une indemnité, les agents doivent avoir occupé des fonctions particulières ou avoir été au service de la Confédération pendant de nombreuses années (art. 78 al. 1 et 2 OPers) et ne pas voir leur contrat résilié pour faute (art. 78 al. 3 let. c OPers). Le montant de l'indemnité est fixé à l'art. 79 OPers et dans l'annexe 3 à l'OPers.

---

224 AUBERT, Commentaire, N 6 *ad* art. 341 CO, p. 2122 ; BONARD, N 15 *ad* art. 335 CO, p. 583.

225 Message LPers, p. 1436.

En cas de convention de départ, l'accord de résiliation est soumis au moins aux mêmes limites que celles qui s'imposent à un même accord relevant du droit privé. Ainsi, les deux parties doivent renoncer à certains droits, de sorte que la transaction n'apporte pas des avantages qu'au seul employeur[226]. La marge de négociation apparaît cependant restreinte compte tenu du principe de la légalité[227].

La convention de résiliation étant un contrat de droit administratif, elle doit s'interpréter selon les mêmes règles que les contrats de droit privé[228] et la question des vices du consentement liés à la conclusion ou à la modification d'un contrat de travail de droit public doit être examinée à la lumière des art. 23 ss CO, applicables par analogie par renvoi de l'art. 6 al. 2 LPers[229].

Le droit cantonal neuchâtelois ne prévoit pas la voie contractuelle pour la fin des rapports de service. Cela ne signifie pas pour autant que le procédé soit exclu sachant qu'il est admis que la conclusion d'un contrat de droit administratif puisse intervenir lorsque la loi ne l'exclut pas[230]. Pour ce qui est des indemnités pouvant être versées, outre celles liées au délai de congé légal, certaines sont prévues en cas de suppression de poste (art. 44 al. 3 et 4 LSt).

Ce qui a été dit plus haut concernant les limites de la convention de départ sous le régime de la LPers vaut à notre sens dans les mêmes termes en cas de convention de départ conclue sous le régime de la LSt.

2. Le principe de transparence

Les conventions de départ sont l'objet de demandes répétées formées au titre de la transparence, en particulier de la part d'organes de presse.

En principe, la demande tendant à connaître la rémunération d'un employé, laquelle comprend également le montant versé dans le cadre d'un départ négocié, doit être refusée afin de respecter sa sphère privée[231]. Une clause de confidentialité, si elle est contenue dans la convention de départ, devrait également faire obstacle à une demande d'accès aux documents fondée sur le principe de la transparence. Toutefois, la jurisprudence du Tribunal administratif fédéral et celle de la Cour de droit public du Tribunal cantonal neuchâtelois apportent quelques nuances.

---

226 TAF A-1711/2014 du 8 décembre 2015, c. 3.3.
227 Dans le même sens, HELBLING, N 17 *ad* art. 34 LPers.
228 TAF A-1711/2014 du 8 décembre 2015, c. 4.
229 TAF A-1711/2014 du 8 décembre 2015, c. 5.
230 TANQUEREL, p. 336.
231 Voir *supra* II.B.

Le Tribunal administratif fédéral a ainsi ordonné la transmission des contrats de travail de deux collaborateurs du Département fédéral de justice et police à un journaliste qui en avait fait la demande, ainsi que des décisions relatives à leur indemnisation après leur renvoi par la nouvelle cheffe du département[232]. Le Tribunal administratif fédéral a commencé par rappeler qu'en principe la demande tendant à consulter le dossier d'un employé doit être refusée afin de respecter sa sphère privée. Mais il relève ensuite que les données purement financières ne sont pas des données sensibles au sens de l'art. 3 let. c LPD, que leur divulgation n'aurait pas de conséquences importantes pour les deux collaborateurs et que l'un d'eux y a même consenti. Puis il considère qu'au vu du contexte politique ayant entouré le départ de ces collaborateurs, le droit d'accéder aux conventions permettra au public de vérifier si les dispositions légales applicables à la résiliation des rapports de service ont correctement été appliquées. Dans ces circonstances particulières, le besoin d'information du public l'emporte sur le droit des intimés au respect de leur sphère privée[233].

Plus récemment, la Cour de droit public du Tribunal cantonal neuchâtelois est parvenue à une conclusion similaire, à la suite d'une demande également formée par un journaliste tendant à l'accès à la convention réglant les modalités de la fin des rapports de service du chef du Service de l'emploi[234]. Elle n'a pas retenu l'objection du Conseil d'État qui soutenait que la transmission de la convention serait de nature à affaiblir sa marge de manœuvre dans d'autres cas futurs similaires[235], et elle a considéré, tout comme l'avait fait le Tribunal administratif fédéral dans l'affaire susmentionnée, que le besoin de protection des données personnelles était moins saillant s'agissant d'un haut cadre de l'administration, dont le départ s'inscrivait également dans une certaine mesure dans un contexte politique[236].

Ces deux précédents ne devraient pas permettre de généraliser l'accès aux conventions de départ conclues par les collectivités publiques. D'ailleurs, le Tribunal fédéral a nuancé la portée de l'intérêt public à la transparence dans ce contexte[237]. Selon le Tribunal fédéral, bien que la protection des données puisse céder le pas devant l'intérêt public à connaître de quelle manière a été réglée un conflit, notamment s'il s'agit d'une personne occupant une haute fonction, l'État peut aussi faire valoir un intérêt à réserver *pro futuro* le secret quant aux modalités de règlement des conflits du travail[238]. Aussi, à notre sens, lorsque le collaborateur n'occupe pas une fonction haut placée et que son départ ne s'inscrit pas dans

232 TAF A-3609/2010 du 17 février 2011.
233 TAF A-3609/2010 du 17 février 2011, c. 5.
234 CDP.2014.23 du 28 janvier 2016.
235 CDP.2014.23 du 28 janvier 2016, c. 4.
236 CDP.2014.23 du 28 janvier 2016, c. 6.
237 TF 1C_273/2015 du 18 septembre 2015.
238 TF 1C_273/2015 du 18 septembre 2015, c. 3.4.1.

un contexte politique, la pesée des intérêts devrait tendre vers la protection de la sphère privée.

Cela étant, il est important de relever que cette dernière affaire concernait non pas une collectivité publique, mais une fondation privée subventionnée par la Ville et l'État dans le canton de Genève. Cet élément a justifié que l'information du public cède le pas sur la protection de la sphère privée, le collaborateur n'étant pas rémunéré directement par l'État, mais par un employeur de droit privé.

VI. Conclusion

Il existe autant de règles qui protègent la confidentialité du salaire que de principes qui en justifient la divulgation. C'est dire qu'il était impossible de répondre de manière péremptoire aux questions que nous avons traitées dans notre contribution. En effet, pour déterminer à quelles conditions l'employeur ou le travailleur sont en droit de communiquer le salaire à des tiers ou pour qualifier la portée d'une clause de confidentialité dans une convention de départ, il faut tout d'abord identifier le *corpus* de règles applicables puis nécessairement opérer une pesée des intérêts en présence.

Dans ce contexte, la démarche n'est pas similaire en droit privé du travail et en droit de la fonction publique, quand bien même la problématique est régie par une même loi fédérale ou des lois cantonales de teneur très proche. La raison en est que la communication du salaire touche aux droits fondamentaux de l'employé. En droit privé du travail, la protection se déploie par la protection des droits de la personnalité des travailleurs, tandis qu'en droit de la fonction publique on raisonne par le prisme de la restriction aux droits fondamentaux. À cela s'ajoute que le principe de la transparence poursuit un intérêt diamétralement opposé.

Il n'en demeure pas moins que dans un domaine comme dans l'autre, l'on doit, pour répondre à la question de la confidentialité du salaire, procéder à une pesée des intérêts. De plus, hormis les particularités propres à chaque régime, les concepts matériels se rejoignent et s'inspirent mutuellement. Nous y voyons un indice supplémentaire des convergences et du rapprochement progressif du droit privé du travail et du droit de la fonction publique[239].

[239] Sur cette question, voir l'ouvrage collectif édité par DUNAND/MAHON/PERRENOUD, récemment publié dans la collection du Centre d'étude des relations de travail (CERT) de l'Université de Neuchâtel.

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.

AUBERSON GÉRALDINE, Personnalités publiques et vie privée – Étude de droit privé suisse à la lumière du droit américain, Genève/Zurich/Bâle 2013.

AUBERT GABRIEL, La protection des données dans les rapports de travail, *in* : Gabriel Aubert et al., Journée 1995 de droit du travail et de la sécurité sociale, Zurich 1999, pp. 145-191 (cité : AUBERT, Protection).

AUBERT GABRIEL, Commentaire des art. 319 ss CO, *in* : Luc Thévenoz/Franz Werro (éds.), Commentaire romand, Code des obligations I, 2e édition, Bâle 2012 (cité : AUBERT, Commentaire).

AUBRY GIRARDIN, Commentaire de l'art. 3 LEg, *in* : Gabriel Aubert/Karine Lempen (éds.), Commentaire de la loi fédérale sur l'égalité, Genève 2011.

BOHNET FRANÇOIS/DIETSCHY PATRICIA, Commentaire de l'art. 341 CO, *in* : Jean-Philippe Dunand/Pascal Mahon (éds.), Commentaire du contrat de travail, Berne 2013.

BONARD ALINE, Commentaire de l'art. 335 CO, *in* : Jean-Philippe Dunand/Pascal Mahon (éds.), Commentaire du contrat de travail, Berne 2013.

BRUCHEZ CHRISTIAN, Réflexions sur l'action judiciaire individuelle pour discrimination salariale, *in* : Jean-Philippe Dunand/Karine Lempen/Pascal Mahon (éds.), L'égalité entre femmes et hommes dans les relations de travail – 1996-2016 : 20 ans d'application de la LEg, Genève/Zurich/Bâle 2016, pp. 179-190.

BRUNNER CHRISTIANE/BÜHLER JEAN-MICHEL/WAEBER JEAN-BERNARD/BRUCHEZ CHRISTIAN, Commentaire du contrat de travail, Lausanne 2004.

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

COMMISSION DES INSTITUTIONS POLITIQUES DU CONSEIL NATIONAL, Rapport relatif à l'Initiative parlementaire « Entreprises liées à la Confédération. Salaire des cadres et rémunération des membres des conseils d'administration » du 25 avril 2002, FF 2002 6972 (cité : Rapport sur le salaire des cadres).

CONSEIL D'ÉTAT DE LA RÉPUBLIQUE ET CANTON DE NEUCHÂTEL, Rapport au Grand Conseil à l'appui d'un projet de loi sur la transparence des activités étatiques du 10 mai 2006 (cité : Rapport LTAE).

CONSEIL D'ÉTAT DE LA RÉPUBLIQUE ET CANTON DE NEUCHÂTEL, Rapport au Grand Conseil à l'appui d'un projet de loi sur la protection des données du 13 août 2008 (cité : Rapport LCPD).

CONSEIL D'ÉTAT DE LA RÉPUBLIQUE ET CANTON DE NEUCHÂTEL, Rapport au Grand Conseil à l'appui d'un projet de décret portant approbation de la convention intercantonale relative à la protection des données et à la transparence dans les cantons du Jura et de Neuchâtel (CPDT-JUNE) et d'un projet de loi portant abrogation de la loi sur la protection des données, du 30 septembre 2008, et de la loi sur la transparence des activités étatiques, du 28 juin 2006, du 9 mai 2012 (cité : Rapport CPDT-JUNE).

CONSEIL FÉDÉRAL, Message concernant la loi sur le personnel de la Confédération du 14 décembre 1998, FF 1998 1421ss (cité : Message LPers).

CONSEIL FÉDÉRAL, Message relatif à la loi fédérale sur la transparence de l'administration du 12 février 2003, FF 2003 1807ss (cité : Message LTrans).

CRAMER CONRADIN, Lohngeheimnis und Lohntransparenz, *in* : PJA 11/2016, pp. 1471-1484.

DANTHE MARIE-GISÈLE, Commentaire des art. 322 à 322d CO, *in* : Jean-Philippe Dunand/Pascal Mahon (éds.), Commentaire du contrat de travail, Berne 2013.

DESSEMONTET FRANÇOIS, Les accords de confidentialité, *in* : François Dessemontet/Paul Piotet (éds.), Mélanges Pierre Engel, Lausanne 1989, pp. 27-37.

DIETSCHY PATRICIA, Les conflits de travail en procédure civile suisse, Bâle 2011.

DUNAND JEAN-PHILIPPE, Commentaire des art. 319, 321a, 321d, 328 et 328b CO, *in* : Jean-Philippe Dunand/Pascal Mahon (éds.), Commentaire du contrat de travail, Berne 2013.

DUNAND JEAN-PHILIPPE, La protection de la personnalité des travailleurs (art. 328 CO) : norme flexible et cardinale du droit suisse du travail, *in* : Margareta Baddeley et al. (éds.), Facettes du droit de la personnalité – Journée de droit civil 2013 en l'honneur de la Professeure Dominique Manaï, Genève/Zurich/Bâle 2014, pp. 47-71 (cité : DUNAND, Protection).

DUNAND JEAN-PHILIPPE/MAHON PASCAL/PERRENOUD STÉPHANIE (éds.), Le droit de la relation de travail à la croisée des chemins : Convergences et divergences entre le droit privé du travail et le droit de la fonction publique, Genève/Zurich/Bâle 2016.

FLÜCKIGER ALEXANDRE/HÄNNI DOMINIQUE, La transparence en matière d'activités accessoires dans les hautes écoles en Suisse, Régimes juridiques et droits d'accès, *in* : Jusletter 3 octobre 2016.

HELBLING PETER, Commentaire des art. 4 et 34 LPers, *in* : Wolfgang Portmann/Felix Uhlmann (éds.), Bundespersonalgesetz (BPG), Berne 2013.

JEANDIN NICOLAS, Commentaire de l'art. 28 CC, *in* : Pascal Pichonnaz/Bénédict Foëx (éds.), Commentaire romand, Code civil I, Bâle 2010.

MALLA JASMIN, Commentaire de l'art. 15 LPers, *in* : Wolfgang Portmann/Felix Uhlmann (éds.), Bundespersonalgesetz (BPG), Berne 2013.

MATTHEY FANNY, Note à propos de l'ATF 136 I 332, *in* : RDAF 2011 I, pp. 363-365.

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

MONTAVON PASCAL, De la confidentialité des données personnelles au sein des entreprises, *in* : Peter Gauch/Franz Werro/Jean-Baptiste Zufferey (éds.), La protection de la personnalité – Contributions en l'honneur de Pierre Tercier pour ses cinquante ans, Fribourg 1993, pp. 75-85.

PORTMANN WOLFGANG/RUDOLPH ROGER, Commentaire des art. 319 ss CO, *in* : Heinrich Honsell/Nedim Peter Vogt/Wolfgang Wiegand (éds.), Basler Kommentar OR I, Bâle 2015.

REHBINDER MANFRED/STÖCKLI JEAN-FRITZ, Commentaire des art. 319 à 330b CO, *in* : Berner Kommentar, Berne 2010.

ROSENTHAL DAVID, Commentaire de l'art. 328b CO, *in* : David Rosenthal/Yvonne Jöhri (éds.), Handkommentar zum Datenschutzgesetz, Zurich/Bâle/Genève 2008.

RUDIN PETER, Commentaire de l'art. 3 LPD, *in* : Bruno Bäriswyl/Kurt Pärli (éds.), Datenschutzgesetz (DSG) - Handkommentar, Berne 2015.

SCHLOSSER RALPH, Les secrets économiques dans les relations de travail, les collaborations et les procès civils, *in* : Jacques de Werra (éd.), La protection des secrets d'affaires, Zurich 2013, pp. 65-91.

STREIFF ULLIN/VON KAENEL ADRIAN/RUDOLPH ROGER, Arbeitsvertrag – Praxiskommentar zu Art. 319-362 OR, 7e édition, Zurich/Genève/Bâle 2012.

SUBILIA OLIVIER/DUC JEAN-LOUIS, Droit du travail – Eléments de droit suisse, Lausanne 2010.

TANQUEREL THIERRY, Manuel de droit administratif, Zurich 2011.

TERCIER PIERRE/BIERI LAURENT/CARRON BLAISE, Les contrats spéciaux, Genève/Zurich/Bâle 2016.

URBEN LUCA, La rémunération des dirigeants en droit suisse de la société anonyme, Lausanne 2015.

WITZIG AURÉLIEN, L'obligation de production de l'employeur et la protection des données des travailleurs ; analyse de l'arrêt du Tribunal fédéral 4A_63/2016, *in* : Newsletter DroitDuTravail.ch janvier 2017.

WYLER RÉMY, Commentaire de l'art. 6 LEg, *in* : Gabriel Aubert/Karine Lempen (éds.), Commentaire de la loi fédérale sur l'égalité, Genève 2011.

WYLER RÉMY/HEINZER BORIS, Droit du travail, 3e édition, Berne 2014.

ANNE-SYLVIE DUPONT*

La protection des données confiées aux assureurs

Sommaire

		Page
I.	Introduction	196
II.	Les données collectées par l'assureur dans le cadre d'une demande de prestations	197
	A. La collecte des données	198
	1. Le cadre légal imposé à l'assureur privé	198
	2. Le cadre légal imposé à l'assureur social	200
	a) Les particularités de l'assurance-invalidité	201
	b) L'assurance obligatoire des soins	202
	3. La collecte des données à l'insu de l'assuré	204
	a) La surveillance ordonnée par l'assureur	204
	b) Autres situations	207
	4. L'expertise médicale	208
	5. Synthèse	210
	B. La gestion des données collectées	211
	1. La gestion des données par les assureurs privés	211
	2. La gestion des données par les assureurs sociaux	213
	a) L'obligation de garder le secret	213
	b) La communication des données	213
	3. Synthèse	217
III.	Et l'employeur ?	218
	A. Au moment de la conclusion des rapports de travail	219
	B. Dans le cadre d'une demande de prestations	221
	1. La collaboration à l'instruction du dossier	221
	2. L'accès au dossier	223
	3. La transmission spontanée d'informations à l'employeur	225
IV.	Conclusion	226
Bibliographie		227

* Je remercie Mme Audrey Voutat, MLaw, avocate, assistante-doctorante à la Faculté de droit de Neuchâtel, qui a effectué les recherches nécessaires à la rédaction de cette contribution, et en a corrigé le manuscrit.

I. Introduction

Parmi tous les secteurs d'activité de l'administration publique et de l'économie libre, *la gestion des assurances, sociales et privées, est sans doute l'un de ceux qui génèrent le volume de données le plus important*. Ces données présentent le plus souvent un caractère très sensible, notamment parce qu'elles ont trait à l'état de santé des personnes assurées. Il en ira ainsi pour pratiquement toutes les assurances sociales, et pour les assurances privées dites de personnes, soit les assurances qui offrent une couverture lorsque le risque assuré se réalise sur la personne assurée[1].

La collecte et la gestion de données par les assureurs, en particulier leur transmission, font l'objet d'un *cadre légal* composé non seulement de la loi fédérale sur la protection des données[2], mais aussi par des dispositions contenues dans le corpus des textes régissant les assurances sociales. L'objet de cette contribution est dans un premier temps de mesurer l'efficacité de ce cadre (II).

Il est ensuite intéressant de préciser, dans ce contexte, la *posture de l'employeur* qui, parfois, se trouve « pris en sandwich » entre son employé et les assurances sociales, respectivement un assureur privé, soit du fait des données qu'il détient et dont il se demande s'il doit ou non les transmettre, soit, à l'inverse, parce qu'il s'interroge sur ses possibilités d'accéder aux données traitées par les assureurs (III).

Nous avons choisi de limiter notre contribution aux *données traitées par les assureurs à la suite d'une demande de prestations*. Nous n'aborderons donc pas, au-delà d'éventuelles allusions, la question des données collectées à l'occasion de la conclusion d'une police d'assurance, ou d'aménagements particuliers des conditions d'assurance pour l'assuré qui accepte de communiquer à l'assureur des données sur ses habitudes de vie[3].

---

1 Cf. FUHRER, N 2.70. Il s'agit par exemple des assurances-vie ou des assurances complémentaires pour les soins de santé.

2 Loi fédérale du 19 juin 1992 sur la protection des données (LPD), RS 235.1.

3 Nous faisons notamment allusion aux rabais de prime consentis aux assurés qui acceptent de communiquer à l'assureur, via des moyens électroniques, l'ampleur de leurs déplacements ou d'autres comportements quotidiens.

II. Les données collectées par l'assureur dans le cadre d'une demande de prestations

Saisi d'une demande de prestations, l'assureur, tant social que privé, doit, afin de se déterminer en connaissance de cause, réunir un certain nombre de données personnelles[4] au sujet de l'assuré. En raison de la nature des risques assurés, qui supposent le plus souvent une atteinte à la santé pour ouvrir le droit aux prestations[5], *les données récoltées sont, dans leur très grande majorité, des données sensibles*[6].

Si l'on se réfère aux règles générales auxquelles obéit la protection de données sensibles de nature médicale, *la situation paraît juridiquement très claire* : « les données ne doivent être transmises à personne, à moins que [l'assuré] ne consente à la communication, qu'une disposition légale n'autorise le transfert de données, voire, exceptionnellement, qu'un autre fait justificatif ne légitime la transmission des informations »[7]. Ainsi, on pourrait penser à première vue qu'il est difficile pour l'assureur d'entrer en possession des données relatives à ses assurés.

Du moment que les données personnelles sont transmises dans le cadre d'une demande de prestations formulée auprès d'un assureur social ou d'un assureur privé, *la relation entre la règle énoncée et ses exceptions se trouve modifiée à cause du rapport de force* existant entre un assuré qui, le plus souvent, a besoin des prestations d'assurance pour survivre, et un assureur qui tient les cordons de la bourse et qui, sans discuter ici de la légitimité de la démarche, s'estime en droit de prendre le temps nécessaire et de se procurer tous les renseignements utiles pour ne les desserrer qu'à bon escient (A).

Une fois les données collectées en revanche, l'assureur, qu'il soit social ou privé, est tenu, dans son rôle de gestionnaire de données, par un cadre légal strict, censé empêcher que les informations recueillies sur l'assuré ne sortent de son giron (B).

---

4 Au sens de l'art. 3 let. a LPD : « toutes les informations qui se rapportent à une personne identifiée ou identifiable ».

5 C'est évidemment le cas dans l'hypothèse du recours à des soins de santé en cas de maladie (art. 3 LPGA) ou d'accident (art. 4 LPGA), mais aussi en cas d'incapacité de travail (art. 6 LPGA) ou d'invalidité (art. 7 et 8 LPGA). Les conditions générales régissant les polices d'assurances privées couvrant ces risques en reprennent très souvent la définition « sociale ».

6 Cf. art. 3 let. c ch. 2 LPD.

7 Cf. GUILLOD, pp. 136 s.

A. La collecte des données

Au stade de la constitution du dossier par l'assureur à la suite d'une demande de prestations, respectivement d'une annonce de sinistre, le cadre légal qui s'impose à lui dépend selon qu'il s'agit d'assurance privée (1) ou d'assurance sociale (2). Dans les deux cas, les contours de la protection des données de l'assuré sont déplacés lorsqu'elles sont collectées à l'insu de ce dernier (3) ou lorsque l'assuré doit se soumettre à une expertise (4). Se pose en conséquence la question de l'effectivité de la protection légale (5).

1. Le cadre légal imposé à l'assureur privé

Les relations entre l'assureur privé et l'assuré, respectivement le preneur d'assurance ou le bénéficiaire des prestations, relèvent du droit civil. Elles sont formalisées par un *contrat* au sens des art. 1 ss CO[8], soumis au cadre minimal de la loi fédérale sur le contrat d'assurance[9].

L'art. 39 al. 1 LCA consacre l'*obligation de collaborer de l'assuré* en exigeant de lui qu'en cas de sinistre, il fournisse à l'assureur, sur demande, « tout renseignement sur les faits à sa connaissance qui peuvent servir à déterminer les circonstances dans lesquelles le sinistre s'est produit ou à fixer les conséquences du sinistre ». Il peut être convenu, par le biais des conditions générales d'assurance, que l'assuré doive remettre les informations requises dans un certain délai, sous peine d'être déchu de son droit aux prestations. Dans ce cas-là, l'assureur doit au préalable adresser à l'assuré une mise en demeure, lui rappelant les conséquences d'un manquement. Le délai ne court que du moment où cette mise en demeure a été faite[10].

En théorie, l'assuré doit s'acquitter de son obligation en transmettant lui-même les pièces utiles, notamment des rapports médicaux. *En pratique, l'assureur demande en règle générale à l'assuré de délier les médecins du secret médical* à son égard, afin qu'il puisse se renseigner directement auprès d'eux.

Sur le fond, cette pratique présente l'avantage de permettre à l'assureur de s'adresser directement aux médecins pour obtenir les renseignements pertinents pour le traitement du litige en cours. Elle présente en revanche l'inconvénient majeur de *donner pour ainsi dire carte blanche à l'assureur qui, bien souvent, libelle les procurations qu'il fait signer aux assurés en des termes très généraux*. Sont ainsi non seulement déliés du secret médical les

---

8 Le contrat d'assurance prend la forme d'une police qui récapitule les prestations promises par l'assureur et les primes consenties en échange par l'assuré, et de conditions générales d'assurance (CGA), dont les dénominations peuvent être diverses.

9 Loi fédérale du 2 avril 1908 sur le contrat d'assurance (LCA), RS 221.229.1.

10 Art. 39 al. 2 ch. 2 LCA.

médecins, hôpitaux et autres professionnels de la santé qui connaissent le cas de l'assuré, mais sont aussi déliés du secret professionnel les autres assureurs privés, les assureurs sociaux, les services sociaux, l'employeur, etc.

La procuration s'inscrit dans le cadre des art. 4 et 13 LPD. Selon ces dispositions, tout traitement de données doit être licite[11], ce qui suppose qu'il soit justifié par le consentement de la personne concernée[12], par un intérêt privé ou public prépondérant, ou par la loi.

Dans le système de la loi sur la protection des données, le consentement de la personne concernée n'équivaut pas à un blanc-seing en faveur du collecteur de données. Ses démarches doivent respecter le principe de la bonne foi et de la proportionnalité, conformément à l'art. 4 al. 2 LPD et, en conséquence, se limiter au sinistre en cause et aux données pertinentes pour que l'assureur puisse se déterminer sur le droit aux prestations de l'assuré, respectivement du bénéficiaire[13]. Ces principes s'opposent selon nous à ce que l'assuré signe une clause de procuration au moment de la conclusion du contrat, par exemple dans le cadre d'un questionnaire de santé, dont l'assureur se prévaudrait ensuite dans le cadre de sinistres concrets[14].

En pratique, l'assureur a les coudées relativement franches, puisqu'il peut – ce qu'il fait – *refuser de verser les prestations tant que l'assuré n'a pas signé la procuration, ou qu'il l'a signée, mais en en biffant certains termes*[15]. Ainsi, si l'assuré, respectivement le bénéficiaire, n'a pas suffisamment de réserves financières pour faire respecter ses droits, il est très facile pour l'assureur d'accéder à toutes les informations qu'il souhaite avoir, même sans rapport direct avec le cas à traiter.

Le rapport de force entre assureur et assuré, respectivement bénéficiaire, est tel que l'on peut à notre avis *douter de la liberté du consentement donné par voie de procuration au traitement des données médicales*. Selon l'art. 4 al. 5 LPD, « lorsque son consentement est requis pour justifier le traitement de données personnelles la concernant, la personne concernée ne consent valablement que si elle exprime sa volonté librement et après avoir été dûment informée ». Nous sommes d'avis que le consentement n'est en tout cas pas donné librement lorsque l'assureur conditionne le versement de prestations financières

11 Art. 4 al. 1 LPD.

12 De manière intéressante, la loi parle de « victime ».

13 GUILLOD, p. 137.

14 D'un avis contraire, ZITTEL, N 12.17.

15 Cette pratique est rapportée par le Préposé fédéral à la protection des données et à la transparence dans son rapport d'activités n° 22 (2014-2015).

destinées à compenser la perte de revenus consécutive à la réalisation du risque assuré[16] à la signature de la procuration[17].

Ce reproche peut cependant être contourné assez aisément par l'assureur à qui l'on reprocherait le traitement illicite de données. Il pourrait se prévaloir de l'art. 13 al. 2 LPD pour *mettre en avant son intérêt prépondérant, dès lors qu'il s'agit de traiter des données en relation directe avec l'exécution d'un contrat*[18], sans pour autant que cela ne conduise automatiquement à considérer cet intérêt comme prévalant dans le cas d'espèce. L'art. 13 al. 2 let. a LPD limite l'exemple du caractère prépondérant de l'intérêt privé dans le cadre contractuel aux cas dans lesquels « les données traitées concernent le cocontractant ». Cette disposition ne peut dès lors à notre sens pas être invoquée dans l'hypothèse d'une assurance pour autrui, par exemple dans le cadre d'une police d'assurance collective conclue avec l'employeur en faveur de ses employés, pour justifier le traitement des données des tiers bénéficiaires des prestations.

Dans les faits, il semble donc bien que l'assuré, malgré le cadre protecteur de la LPD, soit en réalité le plus souvent contraint de libérer l'accès à ses données, les garde-fous étant faciles à enjamber.

2. Le cadre légal imposé à l'assureur social

La loi fédérale sur la partie générale du droit des assurances sociales[19] encadre l'instruction par l'assureur social de la demande de prestations formulée par l'assuré, respectivement par ses ayants droit. Elle est avant tout caractérisée par l'*obligation faite à l'assuré de collaborer gratuitement à l'exécution des différentes assurances sociales*[20]. Celui qui fait valoir son droit à des prestations doit en particulier fournir gratuitement tous les renseignements nécessaires pour établir ce droit et fixer les prestations dues[21].

Dans ce contexte, *l'assuré a l'obligation d'autoriser toutes les personnes et institutions, notamment les employeurs, les médecins, les assurances et les organes officiels, à fournir*

---

16 Il peut s'agir d'indemnités journalières dans le cadre d'une police collective ou individuelle d'indemnités journalières en cas de maladie, mais aussi, par exemple, de rentes versées en cas d'invalidité dans le cadre d'une assurance-vie.

17 Cf. BAERISWYL, N 65 *ad* art. 4 LPD.

18 Cf. ZITTEL, N 12.84.

19 Loi fédérale du 6 octobre 2000 sur la partie générale du droit des assurances sociales (LPGA), RS 830.1.

20 Art. 28 al. 1 LPGA. La LPGA ne s'applique pas à la prévoyance professionnelle. Dans cette branche d'assurance, l'obligation de collaborer est limitée à l'employeur (cf. art. 11 LPP) et à l'organe de révision (cf. art. 52c LPP). Le règlement de prévoyance peut cependant imposer une telle obligation à l'assuré.

21 Art. 28 al. 2 LPGA.

des renseignements, pour autant qu'ils soient nécessaires pour établir le droit aux prestations[22].

L'assuré qui ne satisfait pas à son obligation de collaborer se voit *sanctionner par un refus de l'assureur* d'entrer en matière sur sa demande de prestations, éventuellement par une décision prise « en l'état du dossier », soit en faisant abstraction d'éléments potentiellement utiles, voire importants, pour se prononcer sur ses droits. Cependant, cette sanction ne peut en principe intervenir que si l'assureur a au préalable adressé à l'assuré une *mise en demeure écrite, lui impartissant un délai pour se conformer à ses obligations et l'avertissant des conséquences juridiques de son défaut de collaboration*[23]. À noter que dans le cadre de son obligation de collaborer, l'assuré peut être contraint de se soumettre aux examens médicaux ou techniques nécessaires et raisonnablement exigibles[24].

Les personnes, instances ou organisations sollicitées par les assureurs sociaux sur la base d'une procuration ou en vertu de la loi *ont l'obligation de livrer les renseignements requis*[25]. Il faut toutefois relever que l'assureur social ne dispose pas de pouvoirs coercitifs à leur encontre. S'ils ne satisfont pas à leur obligation, c'est la personne assurée qui en subira les conséquences, par le biais d'un refus ou d'une réduction des prestations.

a) Les particularités de l'assurance-invalidité

Dans le domaine de l'assurance-invalidité, l'accès par l'assureur aux données de l'assuré est d'autant plus facile que *le dépôt d'une demande de prestations emporte automatiquement libération du secret médical et professionnel* à l'égard de toutes les personnes et instances mentionnées dans le formulaire de demande[26]. Toutes les autres personnes, notamment les employeurs, susceptibles de détenir des informations au sujet de l'assuré et qui ne sont pas formellement mentionnées dans le formulaire de demande sont, de par la loi, libérées du secret médical, respectivement du secret professionnel, à l'égard des organes de l'assurance-invalidité[27].

Contrairement à ce qui prévaut pour les autres branches d'assurances sociales, l'office AI qui instruit la demande n'a pas à adresser de mise en demeure, ni à impartir un délai à l'assuré pour fournir les renseignements demandés. Ainsi, *si ce dernier ne réagit pas « sur*

22 Art. 28 al. 3 LPGA.
23 Art. 43 al. 3 LPGA.
24 Art. 43 al. 2 LPGA.
25 Art. 28 al. 3 *in fine* LPGA.
26 Art. 6a al. 1 de la loi fédérale du 19 juin 1959 sur l'assurance-invalidité (LAI, RS 831.20). Cf. également DUPONT, p. 101.
27 Art. 6a al. 2 LAI.

simple réquisition » de l'office, ce dernier peut clore le dossier et refuser les prestations demandées[28].

b) L'assurance obligatoire des soins

La loi fédérale sur l'assurance-maladie[29] contient des *dispositions très précises* sur les informations que les caisses-maladie sont autorisées à se procurer dans le cadre de l'assurance obligatoire des soins[30]. La particularité réside ici également dans le fait que l'assureur peut, de par la loi et donc sans consentement particulier de l'assuré, s'adresser à un tiers directement, en l'occurrence le fournisseur de prestations, pour obtenir les renseignements dont il a besoin.

L'art. 42 al. 3 LAMal impose en effet au fournisseur de prestations[31] de remettre à l'assureur une *facture détaillée et compréhensible*, de même que *toutes les indications nécessaires lui permettant de vérifier le calcul de la rémunération et le caractère économique de la prestation*[32]. Figurent notamment parmi ces informations les dates du traitement, les prestations fournies et les diagnostics[33]. Ces informations doivent être données au débiteur de la rémunération, soit à l'assuré lui-même dans un système de tiers garant[34] et à l'assureur directement dans un système de tiers payant[35]. En pratique, l'assureur aura dans tous les cas accès à cette facture détaillée, à moins pour l'assuré de renoncer à être remboursé pour les frais qu'il a assumés.

L'assureur-maladie peut exiger des *renseignements supplémentaires d'ordre médical* afin de se déterminer sur son obligation de prester[36]. Cette demande peut aussi intervenir en amont du traitement ou des soins, lorsque l'assureur est sollicité pour une garantie de prise en charge[37]. Dans ce cas, les informations sont en principe transmises pas le médecin

---

28 Art. 7b al. 2 let. d LAI.

29 Loi fédérale du 18 mars 1994 sur l'assurance-maladie (LAMal), RS 832.10.

30 La réglementation de la LAMal l'emporte sur celle de la LPD (ATF 133 V 359 c. 6.4).

31 Cf. art. 35 à 40 LAMal.

32 Dans le domaine de l'assurance obligatoire des soins, l'un des buts de la transmission des données est de permettre la maîtrise des coûts de la santé (cf. MANAÏ, p. 151).

33 Cf. art. 59 al. 1 de l'ordonnance du 27 juin 1995 sur l'assurance-maladie (OAMal, RS 832.102).

34 Cf. art. 42 al. 1 LAMal. Le système du tiers-garant est en principe appliqué aux soins dispensés de manière ambulatoire.

35 Cf. art. 42 al. 2 LAMal. Le système du tiers-payant est en principe appliqué pour les traitements stationnaires.

36 Cf. art. 42 al. 4 LAMal. L'assuré doit alors en être informé, et l'assureur doit le rendre attentif à son droit de ne communiquer ces informations d'au médecin-conseil (art. 59a al. 5 OAMal).

37 Par exemple dans le cadre de l'évaluation des soins requis (art. 8 de l'ordonnance du 29 septembre 1995 sur les prestations de l'assurance des soins [OPAS, RS 832.112.31]), de l'approbation d'un traitement à l'étranger dans le cadre d'un projet pilote (art. 36a OAMal) ou encore de l'autorisation

traitant de l'assuré au médecin-conseil de l'assureur-maladie. Il en ira dans tous les cas ainsi lorsque l'assuré en fait la demande[38].

Tenant compte de la facilité avec laquelle l'assureur-maladie peut ainsi accéder à quantité de données sensibles au sujet de ses assurés, la LAMal a en effet prévu un *filtre par le biais du médecin-conseil*[39].Celui-ci a pour tâche de trier les informations confiées par l'assuré, respectivement par son médecin traitant, et de retenir celles qui doivent être transmises à l'assureur-maladie pour que celui-ci puisse se déterminer à bon escient sur son obligation de prester. Conformément à l'art. 57 al. 4 LAMal, le médecin-conseil « donne son avis à l'assureur sur des questions médicales ainsi que sur des questions relatives à la rémunération et à l'application des tarifs. Il examine en particulier si les conditions de prise en charge d'une prestation sont remplies ». Il ne peut transmettre à l'assureur-maladie que « les indications dont [celui-ci a] besoin pour décider de la prise en charge d'une prestation, pour fixer la rémunération, pour calculer la compensation des risques ou pour motiver une décision », et doit respecter « les droits de la personnalité des assurés »[40].

De son côté, le fournisseur de prestations a l'obligation de transmettre au médecin-conseil toutes les informations utiles à la tâche de ce dernier[41]. Pour pallier une éventuelle carence, le médecin-conseil a la faculté d'examiner lui-même l'assuré[42].

Le médecin-conseil est censé s'acquitter de sa tâche en toute indépendance[43]. Le Tribunal fédéral considère en tout cas de manière systématique que l'institution du médecin-conseil permet de garantir la protection des droits de la personnalité de l'assuré[44]. *Cette position est critiquée*, notamment par le Préposé fédéral à la protection des données et à la transparence, qui a souligné « la difficulté de définir ce qu'on entend par "données médicales" », de même que l'ambiguïté de l'engagement de ne communiquer à l'assureur « que les données qui sont absolument nécessaires pour décider du caractère approprié d'une prestation fournie ». Cet engagement, en effet, laisse au médecin-conseil une liberté d'interprétation relativement large, alors qu'il est confronté, de par sa fonction aux intérêts

d'un médicament hors étiquette (art. 71a OAMal) ou ne figurant pas sur la liste des spécialités (art. 71b OAMal).

38 Cf. art. 42 al. 5 LAMal.

39 Cf. art. 57 LAMal.

40 Cf. art. 57 al. 7 LAMal.

41 Cf. OFSP, Circulaire n° 7.1, 2014 (assureurs-maladie : organisation et processus conformes à la protection des données), p. 8. La teneur de cette circulaire a été confirmée par le Tribunal fédéral (ATF 131 V 178, c. 2.4). Cf. également MONTAVON, p. 242.

42 Cf. art. 57 al. 6 LAMal.

43 Cf. art. 57 al. 5 LAMal.

44 Cf. MONTAVON, p. 244 et les références citées en N 24 et 25.

conflictuels des assureurs, des fournisseurs de prestations et des assurés[45]. Le Préposé a relevé que si l'indépendance du médecin-conseil doit d'abord être réalisée par des mesures organisationnelles, elles ne sont pas suffisantes pour protéger les droits des assurés dans tous les cas[46]. *Des contrôles réalisés tant par l'Office fédéral de la santé publique (OFSP) que par le Préposé ont régulièrement révélé des lacunes au niveau de la protection des données*[47].

Même si le médecin-conseil n'offre pas, à cette heure, une garantie absolue de la protection des données des assurés[48], il faut malgré tout admettre que le filtre d'un organe qui se doit indépendant est un pas important dans cette direction, surtout lorsque cet organe est lui-même soumis au contrôle d'instances supérieures ou indépendantes.

3. La collecte des données à l'insu de l'assuré

a) La surveillance ordonnée par l'assureur

L'art. 43 LPGA confère une très grande latitude à l'assureur social qui instruit un dossier à la suite d'une demande de prestations. Selon cette disposition, il « prend d'office les mesures d'instruction nécessaires et recueille les renseignements dont il a besoin ». Peut notamment faire partie des mesures d'instruction nécessaires *le recours à la surveillance par un détective privé*[49].

Cette pratique, critiquée de longue date par la doctrine en raison notamment de l'insuffisance du cadre légal[50], a subi un revers important en octobre 2016. Dans une affaire concernant le droit aux prestations de l'assurance-accidents obligatoire, *la Cour européenne des droits de l'Homme a condamné la Suisse pour violation de l'art. 8*

---

45 Cf. Rapport d'activité du Préposé fédéral à la protection des données et à la transparence, n° 16 (2008/2009), p. 62 s. Cf. également MONTAVON, p. 245.

46 Cf. Rapport d'activité du Préposé fédéral à la protection des données et à la transparence, n° 16 (2008/2009), p. 63.

47 Cf. Rapport d'activité du Préposé fédéral à la protection des données et à la transparence, n° 16 (2008/2009), p. 64 ss ; Rapport d'activité du Préposé fédéral à la protection des données et à la transparence, n° 15 (2007/2008), pp. 63 ss et p. 66.

48 Cf. également MANAÏ, p. 156 s.

49 Sur cette question, en particulier sur la licéité de la preuve, cf. MOSER-SZELESS, pp. 135 ss. Un détective privé est également souvent engagé après l'octroi de prestations, lorsque l'assureur a des doutes sur le bien-fondé du maintien de ces dernières. En matière d'assurance-invalidité, l'art. 59 al. 5 LAI autorise expressément les offices AI à faire appel à des « spécialistes » pour lutter contre la perception indue de prestations, par quoi il faut notamment comprendre les détectives privés (cf. CHAPPUIS, p. 129 et la référence citée en note 75).

50 Cf. MOSER-SZELESS, pp. 140 ss.

CEDH[51], retenant que dans le cas d'espèce, la surveillance de l'assurée par un détective privé constituait une violation de la sphère privée de la recourante qui ne reposait pas sur une base légale suffisante.

La Cour a retenu que si la législation suisse permettait bel et bien aux assureurs sociaux de procéder aux enquêtes nécessaires lorsque l'assuré rechignait à livrer les informations demandées, *les bases légales existantes étaient insuffisamment précises* dans la mesure où elles n'indiquent pas les modalités de la surveillance autorisée (moment, durée), pas plus qu'elles ne prévoient des garanties contre les abus, « par exemple des procédures à suivre lorsque les compagnies stockent, consultent, examinent, utilisent, communiquent ou détruisent des informations ». Il en résulte « un risque d'accès et de divulgation non autorisés d'informations »[52]. Il est important de souligner que dans la présente affaire, la surveillance avait été effectuée sur le domaine public.

À la suite de cet arrêt, *les assureurs sociaux ont, officiellement à tout le moins, cessé de mettre en œuvre des mesures de surveillance par détectives privés*[53], dans l'attente de l'adoption d'une base légale encadrant cette pratique[54]. Cette base légale devrait être intégrée dans la LPGA à l'occasion de sa prochaine révision[55].

Il se pourrait que l'on se souvienne à cette occasion de la proposition formulée par le Conseil fédéral en 2008, à l'occasion d'une première tentative de révision de la loi sur l'assurance-accidents (LAA). Il s'agissait d'*introduire dans la LPGA un article 44a précisément consacré au sujet de la surveillance*. Cette disposition avait la teneur suivante[56] :

> **Art. 44a Surveillance**
>
> [1] La personne qui requiert ou qui bénéficie d'une prestation d'assurance peut faire l'objet d'une observation à son insu si :

---

51 Convention de sauvegarde des droits de l'homme et des libertés fondamentales (CEDH), RS 0.101.

52 Cf. arrêt CourEDH *Vukota-Bojic c. la Suisse* du 18 octobre 2016, requête n° 61838/10. Les traductions entre guillemets sont reprises du communiqué publié le 18 octobre 2016 par la plateforme d'information humanrights.ch.

53 Cf. communiqué de presse de la Suva du 20 octobre 2016, disponible sur son site Internet (http://www.suva.ch), sous la rubrique « La Suva », puis « Médias ».

54 La Suva est intervenue auprès du Parlement pour que cette base légale soit créée rapidement (cf. dépêche de l'ats publiée notamment dans la Tribune de Genève du 22 novembre 2016).

55 L'ouverture de la consultation est annoncée pour le mois de février 2017 (cf. http://www.admin.ch, mis à jour sur le sujet le 5 décembre 2016).

56 Cf. Message du Conseil fédéral relatif à la modification de la loi fédérale sur l'assurance-accidents (Assurance-accidents et prévention des accidents ; organisation et activités accessoires de la CNA) du 30 mai 2008, FF 2008 4877 (4926).

a. l'assureur a des soupçons reposant sur des faits déterminés que cette personne a obtenu ou tente d'obtenir illégalement des prestations; et si

b. les mesures prises jusqu'alors dans le cadre de l'instruction n'ont pas abouti ou les recherches n'auraient aucune chance d'aboutir ou seraient excessivement difficiles.

[2] L'ouverture de l'observation est inscrite au dossier avec indication des faits motivant les soupçons.

[3] L'observation ne peut être menée que sur le domaine public. Elle peut inclure l'usage de moyens d'enregistrement d'images.

[4] Les données récoltées sont mises au dossier. Elles sont détruites au plus tard après 10 jours si elles ne corroborent pas les soupçons.

[5] L'assureur peut charger de l'observation un tiers.

[6] Il informe la personne concernée de l'observation une fois celle-ci levée.

Cette disposition a disparu de la deuxième mouture de la révision de la LAA, qui est entrée en vigueur au 1er janvier 2017[57]. Dans la mesure où elle prévoit de manière assez claire les conditions auxquelles une surveillance peut être ordonnée, postule en particulier son caractère subsidiaire, et indique les modalités de sa réalisation et la durée de conservation des données, *il s'agit vraisemblablement d'une base légale suffisante au sens de l'art. 8 CEDH et de l'art. 36 al. 1 Cst*[58]. Sans doute serait-il préférable, pour s'en assurer, d'y ajouter l'énumération des moyens de surveillance admis[59].

L'arrêt *Vukota-Bojic c. la Suisse* a été rendu dans une affaire concernant un assureur social, qui permettait dès lors l'invocation de la violation de droits fondamentaux, en l'espèce le droit au respect de la vie privée[60]. *Lorsque la surveillance est ordonnée par un assureur privé*, dans un cadre contractuel, sa licéité doit être examinée dans le cadre des art. 28 ss du Code civil[61], qui protègent l'individu contre les atteintes illicites à sa personnalité. Cela suppose, en premier lieu, que l'on soit en présence d'une atteinte à la personnalité de l'assuré, ce qui sera notamment le cas lorsque celui-ci est photographié à son insu[62]. L'atteinte à la personnalité doit en outre être illicite. L'illicéité est admise par principe,

57 Cf. FF 2015 6525 ss.
58 Constitution fédérale de la Confédération suisse (Cst.) du 18 avril 1999, RS 101.
59 Cf. également MOSER-SZELESS, pp. 145 s.
60 Art. 8 CEDH. Cf. également art. 13 Cst.
61 Code civil suisse du 10 décembre 1907 (CC), RS 210.
62 Cf. ATF 136 III 410 c. 2.2.2.

mais peut être levée si elle est justifiée par le consentement de la victime, par un intérêt prépondérant privé ou public, ou par la loi[63].

L'existence d'un intérêt privé prépondérant est assez largement admise par les tribunaux lorsqu'il s'agit pour l'assureur de vérifier que les prestations servies le sont à juste titre[64]. Des critères ont toutefois été posés pour encadrer cette pratique. Ainsi, le rapport entre l'intensité et la durée de la surveillance et le montant des prestations servies doit être proportionné. Il doit en outre exister des indices laissant penser que l'assuré tenterait de percevoir des prestations auxquelles il n'a pas droit en réalité. Finalement, la surveillance ne peut concerner que des faits se déroulant dans des lieux publics, accessibles à tous. Dans tous les cas, la surveillance doit conserver un caractère exceptionnel[65]. D'une manière générale, la licéité de la surveillance des assurés par des détectives est, dans le cadre de l'assurance privée, en principe facilement validée par les tribunaux.

b) Autres situations

Outre la surveillance par des détectives privés, il existe d'autres situations dans lesquelles la licéité des données récoltées fait débat, et, en conséquence, leur utilisation dans le cadre de l'instruction du dossier de l'assuré.

Ainsi, dans une affaire de 2011[66], le Tribunal fédéral devait, dans une cause en matière d'assurances sociales, se prononcer sur l'utilité de joindre au dossier AI, en application de l'art. 43 LPGA, les enregistrements d'une caméra de surveillance installée par un employeur pour surveiller ses employés suspectés de vol. Ces enregistrements avaient été écartés par les autorités pénales en raison de leur illicéité. Notre Haute Cour a estimé ne pas être liée, dans le cadre du volet assécurologique de l'affaire[67], par la décision du juge pénal. *Sous l'angle de la proportionnalité, elle a admis la licéité des enregistrements vidéo du fait de l'intérêt prépondérant de la collectivité des assurés à ne pas financer des prestations indues*[68].

---

63 Art. 28 al. 2 CC.

64 La justification n'est cependant pas automatique (cf. WERMELINGER, N 12 *ad* art. 13 LPD).

65 Cf. CHAPPUIS, p. 126 et les références citées en notes 60 à 64 ; ZITTEL, N 12.95 ss.

66 TF 9C_785/2010 du 10 juin 2011.

67 A la suite de l'enquête pénale, un des employés avaient développés d'importants troubles psychiques qui avaient conduit à une incapacité de travail et à la demande de prestations de l'assurance-invalidité.

68 La base légale justifiant l'enregistrement était, selon le Tribunal fédéral, l'art. 26 al. 2 de l'ordonnance 3 du 18 août 1993 relative à la loi sur le travail (OLT 3, RS 822.113).

4. L'expertise médicale

Dans le cadre de l'instruction du dossier par l'assureur social, celui-ci a la faculté de mettre en œuvre une *expertise externe*, c'est-à-dire réalisée par un médecin ou par un centre d'expertise qui, fonctionnellement, ne fait pas partie de l'organisation de l'assureur[69]. L'assureur privé fonctionne de la même manière[70]. En l'absence de disposition dans ses conditions générales qui obligerait l'assuré à s'y soumettre, l'assureur privé peut exiger qu'il le fasse en mettant en avant son intérêt privé prépondérant, dans le cadre de l'art. 28 al. 2 CC[71].

L'expert externe mandaté par l'assureur est un médecin. À ce titre, il est *soumis au secret médical*. Cependant, dans la mesure où il est ici mandaté par l'assureur, l'assuré est informé que « toutes les informations recueillies au cours de l'expertise seront communiquées au mandant »[72], et la signature d'une procuration dans ce sens lui est demandée.

De fait, l'expert externe ne joue en aucun cas le rôle de filtre que peut assumer le médecin-conseil dans le domaine de l'assurance-maladie. *Toutes les informations communiquées par l'assuré pendant la durée de l'expertise sont ainsi susceptibles d'être transmises à l'assureur*, sans égard pour leur utilité pour l'analyse médicale du cas ni, par répercussion, sur la situation assécurologique[73]. Le tri des données communiquées par l'assuré ne paraît pourtant pas une tâche insurmontable, en particulier lorsque l'assuré présente une atteinte physique objectivable. Par exemple, si l'expert est mandaté pour investiguer l'impact de troubles rhumatologiques ou orthopédiques simples sur la capacité de travail de l'assuré, il n'a à notre sens pas à rapporter, dans l'anamnèse, des pathologies totalement indépendantes et sans lien possible avec l'affection présente. Il en ira de même, en principe, d'une grande partie des données personnelles de l'assuré, comme sa confession, son appartenance politique, un éventuel grade militaire ou l'existence de dettes[74].

---

69 Cf. art. 44 LPGA.

70 Le cadre légal de l'art. 10a LPD doit alors être respecté. Lorsque l'expertise est mise en œuvre par un assureur responsabilité civile, voir le mode opératoire proposé par le Préposé fédéral à la protection des données et à la transparence (http://www.leprepose.ch, rubrique Documentation > Protection des données > Feuillets thématiques).

71 En pratique, il est rare que l'assureur ait à prendre l'initiative d'une procédure, le simple fait de couper les prestations ayant en général un effet positif suffisant sur la volonté de l'assuré.

72 Cf. Lignes directrices de qualité des expertises psychiatriques dans le domaine de l'Assurance-invalidité, établies par la Société suisse de psychiatrie et psychothérapie (SSPP) en février 2012 (annexe 1), p. 23.

73 Sur l'inutilité de la transmission de l'anamnèse dans le domaine de l'assurance obligatoire des soins en particulier, cf. MONTAVON, pp. 249 ss.

74 En revanche, des données propres à son physique, comme le sexe, l'âge et le poids paraissent a priori indispensables à n'importe quelle évaluation médicale.

Nous concédons qu'il est plus difficile, peut-être impossible, de sérier les données « utiles » des données « inutiles » *dans le cadre d'une expertise psychiatrique ou d'une expertise pluridisciplinaire incluant un volet psychiatrique*. En effet, dans le cadre de l'évaluation des limitations fonctionnelles induites par les troubles psychiques diagnostiqués, ou encore pour comprendre le fonctionnement de l'assuré, il est indispensable d'avoir une appréhension complète de la personnalité de l'expertisé.

Ainsi, selon les Lignes directrices émises par la Société suisse de psychiatrie et de psychothérapie, on procédera, pour les besoins de l'expertise, non seulement à une anamnèse systématique, psychiatrique et somatique, incluant notamment la consommation de psychotropes, la sexualité, mais on établira encore (par exemple) :

- l'anamnèse familiale/hérédité ;
- les événements particuliers à la naissance, le développement dans la petite enfance, les relations au sein de la famille, les comportements particuliers durant l'âge préscolaire et scolaire ;
- la carrière scolaire et professionnelle, les activités bénévoles, le service militaire ;
- les activités professionnelles et postes occupés, les dates et les circonstances de l'interruption de l'activité professionnelle, une expérience éventuelle de mesures de réadaptation professionnelle ou des essais de reprise du travail ;
- l'anamnèse sociale (par ex. logement, situation financière/endettement, vie de couple, enfants, droit de garde, mesures tutélaires, obligations d'entretien, le cas échéant aussi dans le pays d'origine, réseau relationnel et manière d'entrer en relation, gestion du handicap par l'entourage) ;
- le déroulement détaillé et représentatif d'une journée type, l'organisation des loisirs, hobbies, aides nécessaires pour le ménage et dans la vie quotidienne, moyens de transport utilisés, types de déplacement, voyages de vacances, etc.
- les événements de vie marquants, cas échéant les infractions commises antérieurement (par ex. à la loi sur la circulation routière).

Toutes ces informations seront transmises à l'assureur avec le rapport d'expertise, et non les conclusions qu'en tirent les médecins uniquement[75]. Nous insistons ici sur le fait que ces données sont transmises aux organes administratifs de l'assureur, sans le filtre préalable d'un service médical[76], filtre pourtant possible dès lors que les assureurs sociaux

[75] L'assurance obligatoire des soins fait office d'exception, vu le rôle de filtre joué par le médecin-conseil (cf. MONTAVON, p. 251).

[76] Dans l'assurance-invalidité, en pratique, l'expert envoie son rapport à l'office AI qui instruit le dossier, le gestionnaire du dossier le transmettant ensuite au Service médical régional pour avis. Le rapport d'expertise est ensuite archivé en format électronique, à la suite des autres documents rassemblés. Il

devant instruire des états de fait médicaux ont à disposition leurs propres services qui pourraient remplir cette fonction[77].

5. Synthèse

Contrairement à une opinion répandue dans le grand public, l'assureur, qu'il soit social ou privé, n'a pas totalement la bride sur le cou lorsqu'il s'agit collecter des données au sujet de l'assuré qui s'est adressé à lui pour obtenir des prestations. *Il existe un cadre légal* que les assureurs doivent respecter.

Force est toutefois de constater que le mors législatif n'a pas grand pouvoir pour retenir le cheval qui s'emballe : dans la pondération des intérêts[78], *l'intérêt de la collectivité des assurés sociaux* à ne pas financer des prestations indues, *respectivement l'intérêt de l'assureur privé* à ne pas verser des prestations auxquelles l'assuré n'a pas droit *l'emporte en effet systématiquement sur l'intérêt de l'assuré* à conserver par-devers lui certains pans de son existence.

En toute lucidité, nous devons admettre qu'un détective privé, respectivement l'expert médecin, n'a pas la possibilité de distinguer totalement les informations pertinentes pour l'instruction du droit aux prestations d'assurances des informations non pertinentes. Ainsi, un rapport d'expertise mentionnera généralement, dans l'anamnèse, la nationalité de l'assuré, ses origines, son statut matrimonial ou son orientation sexuelle, quand bien même ces informations n'ont en principe aucune influence sur le droit aux prestations. De même, un rapport de détective privé révélera pas exemple la marque de la voiture de l'assuré, l'adresse de membres de sa famille, l'existence d'une liaison extra-conjugale ou un intérêt pour un loisir ou un engagement dont l'assuré ne souhaite pas parler autour de lui, pour

en va de même dans l'assurance-accidents, où l'avis du médecin d'arrondissement sur le rapport d'expertise n'est requis que dans un deuxième temps, le rapport d'expertise étant par ailleurs joint au dossier de l'assuré.

77 L'assurance-invalidité dispose des services médicaux régionaux (SMR ; cf. art. 59 al. 2 et 2bis LAI), l'assurance-accident des médecins d'arrondissement pour la Suva (http://www.suva.ch/medecin-arrondissement) et de médecins-conseils pour les autres assureurs au sens des art. 68 ss LAA, l'assurance-chômage d'un médecin-conseil (cf. art. 15 al. 3 et 28 al. 5 de la loi fédérale du 25 juin 1982 sur l'assurance-chômage obligatoire et l'indemnité en cas d'insolvabilité [LACI, RS 837.0]). Les assureurs privés recourent également aux services de médecins-conseils. Le cadre de leur collaboration est purement contractuel, sans cadre légal ou institutionnel.

78 Cette pondération s'opère sous l'angle de la proportionnalité postulée par l'art. 36 Cst. lorsqu'il est question d'assurances sociales, et sous l'angle de l'intérêt privé prépondérant exigé par l'art. 28 al. 2 CC dans le cadre d'un rapport d'assurance soumis au droit privé.

des raisons qui lui sont propres et qui ne découlent pas de la volonté d'obtenir des prestations indues[79].

La décision strasbourgeoise d'octobre 2016[80] est un rappel à l'ordre bienvenu. L'adoption prochaine d'une base légale suffisante sous l'angle de l'art. 8 CEDH permettra aux assureurs de reprendre leurs anciennes habitudes, dont il n'est pas certain qu'elles doivent s'en trouver matériellement modifiées. Il s'agira d'être attentif au cadre législatif mis en place et à son respect dans la pratique.

B. La gestion des données collectées

Comme nous l'avons vu au chapitre précédent, les assureurs, privés et sociaux, ont la faculté d'amasser un grand nombre de données dont le degré de sensibilité peut être très élevé. *Il est donc important d'être conscients de ce qu'ils peuvent ou ne peuvent pas faire avec les données collectées*.

Nous examinerons cette question en distinguant entre assureurs privés (1) et assureurs sociaux (2).

1. La gestion des données par les assureurs privés

La gestion des données par l'assureur privé *doit respecter le cadre de la loi fédérale sur la protection des données*[81]. En particulier, les données personnelles ne doivent être traitées que dans le but qui est indiqué lors de leur collecte, qui est prévu par une loi ou qui ressort des circonstances[82].

À cet égard, l'assureur privé doit renseigner le preneur d'assurance avant la conclusion du contrat d'assurance notamment sur le traitement des données personnelles, y compris le but et le genre de banque de données, ainsi que sur les destinataires et la conservation des données[83]. Ces renseignements doivent être en sa possession au moment où il soumet à l'assureur une proposition d'assurance[84].

---

79 Un rapport de détective privé dévoilera par exemple, sous prétexte de retracer l'emploi du temps de l'assuré, la fréquentation d'une loge maçonnique ou d'assemblées politiques, informations qui sont des données qualifiées de sensibles (cf. art. 3 let. c LPD) et qui, en principe, n'ont aucun lien avec la demande de prestations.

80 Arrêt *Vukota-Bojic c. La Suisse* (cf. note 52).

81 Art. 2 al. 1 let. a LPD. Cf. notamment l'art. 6 LPD au sujet de la communication transfrontière.

82 Art. 4 al. 3 LPD.

83 Art. 3 al. 1 let. g LCA.

84 Art. 3 al. 2 LCA.

Les données, à tout le moins les données médicales, ne peuvent en principe pas être transmises à un tiers sans motifs justificatifs[85]. En l'occurrence, *la loi autorise l'assureur privé, dans la mesure où aucun intérêt privé ne s'y oppose, à communiquer des données à l'office AI dans le cadre de la détection précoce instituée par l'art. 3b LAI*. L'objectif de cette démarche est de s'assurer que les organes de l'assurance-invalidité seront informés suffisamment tôt d'une situation d'incapacité de travail qui se prolonge ou qui se répète[86], afin de leur permettre d'intervenir en amont et de prévenir l'invalidité[87].

L'assureur privé doit limiter sa communication aux données nécessaires pour atteindre le but visé[88]. À cet égard, l'art. 3b al. 1 LAI précise que la communication doit mentionner les « données de l'assuré et de la personne ou de l'institution qui fait la communication ». Elle « peut être accompagnée d'un certificat médical d'incapacité de travail ». Cette formulation, assez limitée, exclut à notre sens que l'assureur privé transmette, à ce stade, l'intégralité de son dossier.

Sur le plan technique, la LPD impose à l'assureur privé de prendre les mesures organisationnelles et techniques appropriées pour protéger les données personnelles contre tout traitement non autorisé[89], notamment la transmission à des tiers. Les contours de la notion de « tiers » ne sont pas forcément simples à tracer lorsque la même compagnie d'assurance fonctionne à la fois comme assureur privé (par exemple comme assureur de la perte de gain en cas de maladie) et comme assureur social (par exemple comme assureur-accidents LAA). À notre sens, une limite très nette doit être tracée entre les différentes entités d'un groupe d'assurance, les entités gérant les assurances sociales devant être clairement considérées comme des « tiers » s'agissant de la communication des données. Les mesures commandées par l'art. 7 al. 1 LPD doivent donc également permettre d'étanchéifier les rapports entre les différentes entités du groupe d'assurance[90].

---

85 Art. 12 al. 2 let. c LPD.

86 Le cas d'un assuré peut être signalé à l'office AI si celui-ci présente une incapacité de travail ininterrompue de 30 jours au moins, ou si, en l'espace d'une année, il s'est absenté de manière répétée pour des périodes de courte durée (art. 1er du règlement du 17 janvier 1961 sur l'assurance-invalidité [RAI, RS 831.201]).

87 Cf. art. 3a al. 1 LAI.

88 Art. 39a al. 2 LCA.

89 Art. 7 al. 1 LPD.

90 Dans le même sens, KIESER, N 20 s. *ad* art. 33 LPGA et les références citées. Une séparation rigoureuse serait aussi dans l'intérêt de l'assureur, si l'on se réfère au Tribunal fédéral qui, en 2014, a admis que des faits connus d'un assureur-maladie l'étaient aussi de la compagnie d'assurance privée faisant organisation et administration communes avec lui (même adresse, mêmes lignes téléphoniques, papier à en-tête commun, mêmes collaborateurs), de sorte qu'elle n'était pas fondée à plaider la réticence (TF 4A_294/2014 du 30 octobre 2014).

2. La gestion des données par les assureurs sociaux

Les assureurs sociaux sont, par principe, tenus au secret s'agissant des données récoltées dans le cadre de l'instruction d'un dossier (a). La loi aménage cependant de nombreuses exceptions (b).

a) L'obligation de garder le secret

L'art. 33 LPGA impose aux personnes qui participent à l'application des lois sur les assurances sociales ainsi qu'à son contrôle ou à sa surveillance de *garder le secret à l'égard de tiers*[91]. Le cercle des destinataires de la norme est tracé de manière large, de sorte que toutes les personnes qui participent à la mise en œuvre des assurances sociales en font partie[92]. Il s'agit aussi bien du personnel administratif que médical des assureurs, y compris les experts et centres d'expertise externes, ou encore les établissements médicaux et les centres d'observation professionnelle.

Le devoir de secret s'étend non seulement aux données qui figurent dans le dossier, mais aussi à *tous les faits dont les personnes susmentionnées ont connaissance dans le cadre de leurs fonctions*[93].

L'obligation de garder le secret empêche toute communication à des personnes, institutions ou autorités externes à l'assureur[94]. Au plan interne, les communications doivent être limitées à ce qui est nécessaire pour le bon fonctionnement de l'assurance. Ainsi, on évitera par exemple de communiquer à un employé de l'assureur l'existence d'un dossier ouvert au sujet de l'un de ses proches[95]. Sur le plan technique, on peut douter qu'un système informatique qui permet à tous les collaborateurs, indépendamment de leurs fonctions, d'accéder à l'intégralité des dossiers gérés par l'assurance soit conforme avec l'art. 33 LPGA.

b) La communication des données

L'art. 33 LPGA érige l'obligation de garder le secret en principe général, sans exception apparente. Il ne faut toutefois pas perdre de vue qu'avant l'entrée en vigueur de la LPGA, l'art. 19 al. 1 LPD postulait déjà l'interdiction, pour l'assureur social, de communiquer des

---

91 L'art. 86 de la loi fédérale du 25 juin 1982 sur la prévoyance professionnelle vieillesse, survivants et invalidité (LPP, RS 831.40) est formulé de la même manière et impose les mêmes obligations aux personnes qui participent à l'administration de la prévoyance professionnelle obligatoire.

92 Cf. KIESER, N 18 *ad* art. 33 LPGA.

93 Cf. KIESER, N 19 *ad* art. 33 LPGA.

94 Par exemple les membres de la famille, l'employeur ou un assureur privé.

95 Cf. KIESER, N 23 *ad* art. 33 LPGA et les références citées.

données à l'extérieur, à moins d'une exception prévue dans une loi au sens formel. Pour cette raison, *les lois spéciales en matière d'assurances sociales prévoient toutes des dispositions qui autorisent l'assureur social, dans certains cas, à transmettre les données qu'ils détiennent*[96]. Ces dispositions ont été volontairement conservées après l'entrée en vigueur de la LPGA et n'ont été que légèrement modifiées, dans ce sens qu'on a dû y intégrer la mention expresse d'une dérogation à l'art. 33 LPGA[97].

La LPGA prévoit elle-même, sans toutefois les désigner comme telles, un certain nombre d'exceptions au principe de confidentialité, de même que d'autres lois, en dehors du corpus de textes applicables aux assurances sociales.

– L'art. 31 al. 2 LPGA impose à « toute personne ou institution participant à la mise en œuvre des assurances sociales » d'*informer l'assureur* « si elle apprend que les circonstances déterminantes pour l'octroi de prestations se sont modifiées ». Cette obligation tend non seulement à garantir la saine administration des assurances sociales, mais protège aussi dans une certaine mesure la personne assurée, dont le risque de se voir exposé à une demande de restitution de prestations versées à tort[98] diminue d'autant[99]. L'obligation d'annoncer ne concerne que les modifications « importantes », c'est-à-dire celles dont l'impact sur le droit aux prestations – condition nécessaire – ne peut être qualifié de minime[100] ;
– l'art. 32 LPGA, sous l'étiquette de l'assistance administrative, impose aux organes des différentes assurances sociales de *se prêter mutuellement assistance en se fournissant gratuitement les données* qui leur sont nécessaires pour fixer ou modifier des prestations, ou encore en réclamer la restitution, prévenir des versements indus, fixer et percevoir les cotisations ou encore faire valoir une prétention récursoire contre un tiers responsable. La demande d'assistance doit en principe être formulée par écrit et être motivée[101]. L'énumération des questions sur lesquelles l'assistance administrative peut être demandée exclut à notre sens la remise intégrale du dossier à l'auteur de la demande[102] ;

96 Cf. *infra* b).

97 Cf. KIESER, N 27 s. *ad* art. 3 LPGA.

98 Cf. art. 25 LPGA.

99 Cf. KIESER, N 3 s. *ad* art. 31 LPGA.

100 A titre d'exemple, en matière d'assurance-accidents, une modification du taux d'invalidité de 5 % représente le seuil minimum justifiant une modification « importante », et donc une obligation de l'annoncer (cf. KIESER, N 8 *ad* art. 31 LPGA).

101 Art. 32 al. 1 LPGA. Les lois spéciales peuvent prévoir des cas dans lesquels l'aide doit être fournie même sans demande formelle (cf. art. 50a al. 1 let. b de la loi fédérale du 20 décembre 1946 sur l'assurance-vieillesse, survivants et invalidité [LAVS, RS 831.10] et 82 LAMal).

102 Dans le même sens, cf. KIESER, N 9 *ad* art. 32 LPGA.

– l'art. 47 LPGA aménage un *droit* à certaines personnes autres que l'assuré *de consulter le dossier*, ceci dans la mesure où les intérêts privés prépondérants sont sauvegardés[103]. Il s'agit des parties à une procédure qui entendent exercer un droit ou remplir une obligation découlant d'une loi sur les assurances sociales ou faire valoir un moyen de droit contre une décision fondée sur cette même loi[104], des autorités habilitées à statuer sur les recours contre des décisions fondées sur une loi sur les assurances sociales, pour les données nécessaires à l'accomplissement de cette tâche, et finalement des tiers responsables et son assureur, pour les données qui leur sont nécessaires pour se déterminer sur une prétention récursoire de l'assurance sociale concernée ;
– comme indiqué ci-dessus, les lois spéciales en matière d'assurances sociales permettent la communication des données détenues par les assureurs sociaux, à des conditions différentes en fonction du destinataire des données. Ainsi, les données peuvent en principe être transmises sans condition particulière, à moins de l'existence d'un intérêt privé prépondérant, par exemple aux organes d'exécution du régime d'assurance en question ou des autres régimes d'assurances sociales, aux autorités fiscales, aux autorités pénales lorsqu'il s'agit de dénoncer ou de prévenir un crime, aux organes de la statistique fédérale, au Service de renseignement de la Confédération ou aux organes de sûreté cantonaux. Sur demande écrite et motivée, elles peuvent en outre notamment être transmises aux autorités compétentes en matière d'aide sociale, aux tribunaux civils et pénaux, aux offices des poursuites et aux autorités de protection de l'enfant et de l'adulte[105] ;
– certains fichiers exploités par les différents assureurs sociaux sont librement et directement accessibles par d'autres (*procédure d'appel*[106]). Cette possibilité doit reposer sur une base légale formelle[107]. Les registres auxquels l'accès est garanti

---

[103] Cette condition doit être examinée d'un point de vue objectif par l'organe qui est requis de laisser l'accès au dossier. Il s'agira en premier lieu des intérêts de la personne assurée, mais il se peut aussi qu'il s'agisse de l'intérêt d'un proche parent (cf. KIESER, N 29 s. *ad* art. 47 LPGA).

[104] Cette désignation ouvre un champ assez large : il peut s'agir notamment d'un membre de la famille légitimé à agir, ou de l'employeur (cf. art. 34 LPGA : « Ont qualité de parties les personnes dont les droits ou obligations résultent des assurances sociales, ainsi que les personnes, organisations ou autorités qui disposent d'un moyen de droit contre la décision d'un assureur ou d'un organe d'exécution de même niveau »).

[105] Cf. art. 50a LAVS (auquel renvoient les art. 66a LAI, 29a LAPG et 25 let. b LAFam), 97 LAA, 95a LAM, 97a LACI, 84a LAMal et 86a LPP.

[106] Sur cette notion, cf. VALTERIO, N 3178.

[107] Cf. art. 19 al. 3 LPD. Dans son 17e rapport d'activités (2009/2010), le Préposé fédéral à la protection des données et à la transparence mettait en doute l'existence de bases légales suffisantes pour la communication des données en matière d'AVS/AI (cf. p. 65 s.).

contiennent en principe des données de type administratif, nécessaire à l'administration des différentes assurances sociales[108] ;

– *d'autres dispositions du droit fédéral* peuvent également obliger les organes des différentes assurances sociales à communiquer des informations qu'elles détiennent au sujet d'une personne assurée[109]. Il faut encore mentionner l'art. 19 al. 1 LPD, qui en dehors d'une dérogation prévue par une loi au sens formel, autorise aussi la communication de données dans quatre hypothèses, et notamment si la personne qui demande à accéder aux données rend vraisemblable que la personne concernée ne refuse son accord ou ne s'oppose à la communication que dans le but de l'empêcher de se prévaloir de prétentions juridiques ou de faire valoir d'autres intérêts légitimes; dans la mesure du possible, la personne concernée sera auparavant invitée à se prononcer[110].

En définitive, force est de constater que si le principe de l'obligation de garder le secret semble à première vue ériger une digue suffisamment haute pour que les données récoltées par les assureurs, avec la facilité rappelée ci-dessus[111], soient conservées en lieu sûr, *le nombre et la diversité des situations permettant à ces données de voyager d'un interlocuteur à l'autre ébranlent l'édifice*.

Du fait de l'assistance administrative, *les données peuvent circuler, pour ainsi dire librement, entre les différents assureurs sociaux*, soit dix acteurs principaux, sans compter toutes les personnes et institutions intervenant dans le cadre de chaque volet et qui, en principe, auront librement accès aux données une fois qu'elles se trouveront dans le giron de « leur » assureur social.

Les passerelles vers l'extérieur ne sont pas moins nombreuses, quoique peut-être légèrement mieux surveillées. L'intérêt privé prépondérant peut encore tenter de faire barrage. Dans la mesure où, comme nous l'avons déjà montré plus haut, l'intérêt privé cède le plus souvent le pas, dans les débats relatifs à la protection des données, à l'intérêt public supérieur de la collectivité des assurés de ne pas financer des prestations versées à tort et, plus généralement, à la bonne marche des assurances sociales, nous doutons de l'équité de la pondération des intérêts et, par conséquent, de l'efficacité d'une protection par ce biais-là.

Cette perméabilité ne doit pas être considérée d'un œil négatif exclusivement. *Parfois, elle est utile à l'assuré*, par exemple dans le cadre de la collaboration interinstitutionnelle (CII).

---

108 Par exemple, la Centrale du 2e pilier a accès aux registres de la Centrale de compensation de l'AVS dans la mesure prévue à l'art. 24d al. 3 LPP. Pour d'autres exemples, cf. PRIEUR, N 13.153 ss.

109 Cf. en particulier l'art. 12 de la loi fédérale du 17 juin 2005 sur le travail au noir (LTN, RS 822.41).

110 Art. 19 al. 1 let. d LPD. Cf. p. 30.

111 Cf. *supra* A.

On parle de collaboration interinstitutionnelle pour désigner la collaboration entre plusieurs institutions, notamment dans le domaine de la sécurité sociale. Elle a pour but « l'harmonisation optimale des différents systèmes de sécurité et d'intégration, afin que les offres puissent être utilisées de manière plus efficace dans l'intérêt des personnes soutenues »[112]. Dans ce contexte, c'est-à-dire lorsque l'échange d'information se veut au service de l'assuré et de sa réintégration sociale, le cadre législatif décrit ci-dessus a plutôt l'effet d'une entrave[113].

Nous avons également eu l'occasion de mentionner d'autres exemples dans lesquels *la « transparence » de l'assuré peut aussi jouer en sa faveur*, par exemple en lui évitant de s'exposer à une demande de restitution de prestations indues[114], ou encore en faisant obstacle à l'invocation d'une réticence par l'assureur[115].

Néanmoins, *il n'est pas certain que la perméabilité helvétique trouve grâce aux yeux de la Cour européenne des droits de l'Homme*. Dans une affaire remontant à 1997, la Suède s'était en effet vue condamnée en raison de son système de sécurité sociale permettant le transfert du dossier d'une assurée d'une autorité publique à une autre, un nombre important d'agents publics ayant été en mesure d'en prendre connaissance, alors que le dossier recelait des informations qui, initialement, avaient été collectées dans un autre but que celui de la procédure dans le cadre de laquelle le dossier avait circulé. La Cour avait rappelé que « la législation interne doit ménager des garanties appropriées pour empêcher toute communication ou divulgation de données à caractère personnel relatives à la santé qui ne seraient pas conformes aux garanties prévues à l'article 8 CEDH »[116].

3. Synthèse

En théorie, le cadre imposé aux assureurs sociaux au sujet de la communication des données qu'ils détiennent est de nature à empêcher tout problème, puisqu'ils ont l'obligation de se taire. Les exceptions à ce principe sont cependant à ce point nombreuses qu'en réalité, lorsqu'une information est « dans le circuit » d'un assureur social, elle l'est aussi, virtuellement en tout cas, dans celui de tous les autres.

---

112 Cf. les Principes de base de la collaboration interinstitutionnelle (CII), par le Comité national de pilotage CII (rattaché au Département fédéral de l'Intérieur), 13 décembre 2011.

113 Voir à ce sujet l'avis de droit établi par KURT PÄRLI, publié sous le titre « IIZ-Datenaustausch. Datenschutz und Datenaustausch in der interinstitutionnellen Zusammenarbeit (IIZ) » (cf. bibliographie).

114 Cf. p. 19.

115 Cf. note 90.

116 Arrêt CourEDH *M. S. c. la Suède* du 27 août 1997, requête n° 20837/92, par. 41. Cf. également MANAÏ, pp. 138 s.

La transmission des informations d'un assureur social à un assureur privé suppose l'existence d'une base légale formelle – qui existe parfois – ou, à défaut, le consentement de la personne assurée[117]. Comme nous l'avons vu dans la première partie de cette contribution, le consentement apparent de l'assuré n'est pas difficile à obtenir dès lors qu'il a en principe besoin des prestations d'assurance pour survivre.

Dans l'autre sens, *la transmission d'informations d'un assureur privé à un assureur social* ne sera pas moins facile à obtenir, vu l'obligation de collaborer imposée à l'assuré qui a demandé des prestations.

En acceptant de confier ses données à un assureur, qu'il soit social ou privé, l'assuré doit ainsi admettre qu'elles puissent être mises à disposition d'un nombre important d'intervenants, dont l'identité n'est pas prévisible pour lui, en raison de la complexité de la réglementation légale et de l'absence, la plupart du temps, d'une obligation de l'informer au préalable à ce sujet.

III. Et l'employeur ?

Les explications qui précèdent montrent que les règles qui président à la protection des données dans les rapports entre assureur et assuré sont loin d'être simples. La situation se complique encore lorsqu'intervient l'employeur de l'assuré. Le degré de complication est différent selon le moment auquel le contact entre l'employeur et l'assureur se produit, et selon les motifs de ce contact.

Bien que notre contribution soit limitée à la protection des données confiées à l'assureur dans le cadre d'une demande de prestations (B), nous dirons d'abord quelques mots au sujet des informations dont l'assureur peut avoir connaissance au moment de la création des rapports de travail (A).

Nous ne traiterons en revanche pas de la question de la communication par l'employeur à l'assureur, pendant la durée des rapports de travail, des données relatives à la bonne marche des assurances[118].

---

[117] Cf. art. 19 al. 1 LPD.

[118] Par exemple la communication des salaires à la caisse de compensation, à l'institution de prévoyance ou aux assureurs privés en vue de la fixation des cotisations ou de la prime. Les obligations de l'employeur à cet égard sont expressément prévues par la loi ou par le contrat.

A. Au moment de la conclusion des rapports de travail

Il ne s'agit pas de traiter ici des informations que l'employeur est en droit ou non de se procurer, lors de la procédure de recrutement, notamment par les questions qu'il pose lors de l'entretien d'embauche pour fonder sa décision d'engager tel ou tel travailleur. Cette question relève en effet exclusivement du droit du travail[119].

Il arrive en revanche que l'employé, au moment de son engagement, doive *fournir des informations d'ordre médical, en vue de son affiliation à certaines assurances*[120]. De par leur nature, ces informations sont destinées à l'assureur, afin qu'il puisse se déterminer sur le principe, respectivement sur l'étendue de l'affiliation du travailleur. S'agissant de données sensibles[121], ces informations n'ont pas à être communiquées à l'employeur. Un éventuel consentement de l'employé, invoqué à titre de motif justificatif, devrait selon nous être considéré avec une grande prudence. En effet, il n'est pas exclu qu'au moment de la conclusion du contrat de travail, le futur employé subisse une certaine pression due à l'espoir d'être engagé, qui pourrait le pousser à consentir à remettre à l'employeur des données sensibles le concernant. À notre sens, il est indispensable d'éviter tout quiproquo à ce sujet, soit en laissant le soin à l'assureur de communiquer directement avec l'employé, soit en attirant clairement l'attention du travailleur sur le fait que les questionnaires de santé ne doivent pas être adressés à l'employeur, mais à l'assureur directement, plus précisément au service de son médecin-conseil, par exemple en remettant à l'employé une enveloppe réponse.

Si la communication des données à l'assureur conduit à une admission sans réserve, il n'y a aucune raison valable pour que l'employeur ait connaissance des informations communiquées au moment de la conclusion du contrat de travail. Il peut en aller différemment *si, sur la base du questionnaire de santé, l'assureur a refusé d'admettre l'employé, ou s'il a limité la couverture par le biais d'une réserve*. Le droit de l'employeur d'accéder à ces informations dépend à notre sens de l'impact de la décision de l'assureur sur ses propres obligations à l'égard du travailleur :

---

119 Sur cette thématique, cf. CARUZZO, N 2 ss *ad* art. 328b CO.

120 Il s'agira principalement de l'assurance collective d'indemnités journalières (LCA), de la prévoyance professionnelle surobligatoire (art. 331 ss CO) et de l'assurance-accidents complémentaire (LCA). *Sur la question particulière du « mélange des genres »* lorsque l'employeur exploite une caisse d'entreprise ou dispose d'une institution de prévoyance autonome, cf. PÄRLI, *REAS*, p. 35. Ces situations sont à notre sens comparables à celles que l'on trouve dans la *fonction publique*, lorsque l'employeur verse le salaire en cas d'incapacité de travail sans recourir à une couverture d'assurance, cas échéant avec l'intervention de la caisse publique de pension, ou encore lorsque l'employeur est précisément la compagnie d'assurance auprès de laquelle l'employé est assuré.

121 Cf. art. 3 let. c ch. 2 LPD.

– dans le cadre de la *prévoyance surobligatoire*, une exclusion de la couverture ou une limitation par le biais d'une réserve est sans effet pour l'employeur. Ses obligations à l'égard de son employé ne s'en trouvent pas accrues, et il n'y a pas d'impact sur les primes à payer. Dans ce cas, l'employeur ne peut se prévaloir d'un intérêt à la communication de la décision de l'institution de prévoyance, et encore moins des données sensibles à la base de cette décision[122] ;
– dans le cadre de l'*assurance collective d'indemnités journalières en cas de maladie*, en revanche, la décision de l'assureur a un impact direct sur les obligations de l'employeur qui, en l'absence de couverture, voit renaître son obligation de verser le salaire en cas d'empêchement non fautif de travailler[123]. A notre avis, *on ne peut en déduire sans autres un intérêt prépondérant de l'employeur à se voir communiquer par l'assureur le résultat de son appréciation*. Au début des rapports de travail, en particulier pendant le temps d'essai, le délai de résiliation du contrat est le plus souvent extrêmement bref[124]. Dans le même temps, l'obligation de verser le salaire en cas d'incapacité de travailler non fautive reste de courte durée[125], voire n'existe pas[126]. À ce moment de la relation contractuelle, l'intérêt de l'employé à la non-information de son employeur l'emporte ainsi clairement sur l'intérêt de l'employeur à être renseigné. *Le rapport entre les deux intérêts individuels s'inversera avec la durée des rapports contractuels* et l'augmentation, en particulier, de la durée durant laquelle l'employeur devra verser le salaire en cas d'empêchement de travailler[127]. Dans tous les cas, si l'employeur peut faire valoir un intérêt prépondérant à connaître l'existence, respectivement l'ampleur de la couverture d'assurance, il n'a en principe pas d'intérêt à connaître la nature de l'atteinte à la santé qui a conduit à une exclusion ou à l'instauration d'une réserve[128] ;
– dans le cadre d'une *assurance complémentaire à l'assurance-accident sociale*, la situation de l'employeur n'est pas impactée par le refus de couverture ou la réserve imposée par l'assureur. Il ne peut donc pas invoquer d'intérêt prépondérant à se voir communiquer le résultat de l'évaluation de l'assureur.

122 Cf. PÄRLI, *REAS*, p. 35.
123 Cf. art. 324a CO.
124 Cf. art. 335b al. 1 et 335c al. 1 CO.
125 Cf. art. 324a al. 2 CO.
126 Cf. art. 324a al. 1 CO.
127 Dans le même sens, PÄRLI, *REAS*, p. 35.
128 Dans le même sens, CARUZZO, p. 329, qui critique la pratique actuelle des assureurs qui communiquent leurs décisions en double à l'employeur.

B. Dans le cadre d'une demande de prestations

Lorsqu'un sinistre est survenu, respectivement lorsqu'un risque social s'est réalisé et que le travailleur a demandé des prestations à l'assureur privé ou social, se pose tout d'abord la question de savoir dans quelle mesure l'employeur peut, respectivement doit, collaborer à l'instruction du dossier par l'assureur, notamment en lui transmettant des informations au sujet de son employé (1). Se pose ensuite la question de savoir si l'employeur peut accéder au dossier constitué par l'assureur, social ou privé (2). Finalement, on peut encore se demander si certaines circonstances justifient que l'assureur transmette certaines informations à l'employeur en vue de préserver les intérêts de ce dernier, même sans demande de sa part (3).

1. La collaboration à l'instruction du dossier

En matière d'assurances sociales, *l'employeur est tenu, au même titre que l'assuré, de collaborer gratuitement à l'exécution des différentes assurances sociales*[129]. Il est habilité à transmettre les informations nécessaires pour établir le droit aux prestations dès lors que l'assuré, de son côté, est tenu de l'y autoriser[130]. L'employeur peut, cas échéant, être amené à remplir lui-même un formulaire de demande de prestations[131]. Il est alors tenu de répondre avec exactitude aux questions qui lui sont posées.

Dans les formulaires de demande de prestations, ou dans les formulaires servant à obtenir des informations complémentaires de sa part, *l'employeur est en principe questionné sur des données qui sont de son ressort et qu'il est autorisé à traiter*[132]. Leur transmission est justifiée par un intérêt privé prépondérant de l'employé, puisque le versement des prestations dépend des informations que l'employeur transmettra.

Les questions contenues dans les formulaires des assureurs, en particulier celles qui concernent des données sensibles, à l'image des questions sur l'état de santé de l'assuré, *respectent en principe le principe de proportionnalité* :

– *en matière d'assurance-chômage*, l'employeur doit indiquer sur l'attestation de l'employeur si l'employé a été empêché de travailler durant le délai de congé ou si, au cours des 12 derniers mois, il y a eu des périodes d'absence en raison de maladie ou

---

129 Art. 28 al. 1 LPGA.

130 Art. 28 al. 3 LPGA.

131 Art. 29 al. 2 LPGA.

132 Par exemple les derniers salaires touchés, le taux d'occupation, l'identité de celui qui a résilié le contrat de travail, etc. 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 ».

d'accident[133]. L'employeur doit cependant se limiter, cas échéant, à indiquer les dates concernées. Il n'est pas interrogé sur l'affection présentée par son employé ;

– *dans l'assurance-invalidité*, le questionnaire envoyé à l'employeur ne demande pas non plus à ce dernier de livrer des informations sur la nature de l'atteinte à la santé présentée par l'employé. Il est également questionné sur les données salariales, y compris sur l'existence d'un salaire de substitution (indemnités journalières LCA ou LAA), sur le rendement effectif du travailleur et sur les dates des périodes d'incapacité de travail[134] ;
– *dans le cadre de l'assurance-accidents obligatoire*, le lien entre l'assureur et l'employeur est plus étroit, donc plus flou. La loi oblige en effet le second à informer le premier sans retard dès qu'il apprend que l'un de ses employés a été victime d'un accident qui nécessite un traitement médical et/ou provoque une incapacité de travail[135]. L'assureur doit mettre à la disposition de l'employeur les formulaires nécessaires, soit sous format papier, soit sous format électronique[136]. De son côté, « l'employeur doit fournir à l'assureur tous les renseignements nécessaires, tenir à sa disposition les pièces servant à établir les circonstances de l'accident et donner aux mandataires de l'assureur libre accès aux locaux de l'entreprise »[137].

  De fait, *les formulaires de déclaration d'accident interrogent le plus souvent l'employeur sur les blessures subies*. Les informations demandées sont toutefois très succinctes : l'employeur est interrogé sur la partie du corps qui a été touchée et la nature de la lésion. L'employeur n'est pas nécessairement informé de ces éléments et peut renvoyer la déclaration d'accident en laissant cette rubrique en blanc s'il ne possède pas les informations nécessaires[138]. Dans tous les cas, cette question n'autorise à notre sens pas l'employeur à mentionner un diagnostic, ni à faire d'autres commentaires au sujet de l'état de santé de son employé[139].

---

133 Questions 12 et 18 de l'attestation de l'employeur, disponible sur le site Internet http://www.espace-emploi.ch.

134 Cf. Questionnaire pour l'employeur : Réadaptation professionnelle/Rente, disponible sur le site Internet http://www.avs-ai.ch.

135 Art. 45 al. 2 LAA.

136 Cf. Guide de l'assurance-accidents obligatoire LAA, édité par l'Association suisse d'assurances, 3e version, juin 2004, p. 27.

137 Art. 56 de l'ordonnance du 20 décembre 1982 sur l'assurance-accidents (OLAA, RS 832.202).

138 Cf. la fiche explicative « Déclaration des accidents et des maladies professionnelles. Surveillance de l'évolution du cas. Paiement de l'indemnité journalière », établie par la Suva (réf. : 451.f), ch. 1.4.

139 Par exemple en faisant allusion à d'autres atteintes à la santé présentée par le travailleur avant l'accident.

En tant que « personne ou institution participant à la mise en œuvre des assurances sociales »[140], l'employeur a l'obligation d'informer l'assureur s'il apprend que des circonstances déterminantes pour l'octroi de prestations se sont modifiées, si l'assuré retarde sa guérison en ne se présentant pas régulièrement chez le médecin ou en en se conformant pas à ses prescriptions, ou encore s'il ne reprend pas le travail malgré l'ordre du médecin[141]. Dans ce sens, l'employeur doit être considéré comme un véritable auxiliaire de l'assureur-accidents dans la mise en œuvre de cette assurance sociale. À notre sens, cela ne lui confère toutefois pas un pouvoir plus large, s'agissant de la transmission de données sensibles en particulier, que celui qui s'inscrit dans les limites des principes définis dans la loi sur la protection des données, en particulier le principe de proportionnalité.

Dans le domaine de l'assurance privée, les éventuelles obligations de l'employeur doivent être définies dans les conditions générales. Si elles ne prévoient rien, il est d'usage, comme nous l'avons indiqué plus haut, que l'assureur obtienne de l'assuré, au moment de l'ouverture du dossier, la signature d'une procuration qui autorise un certain nombre de personnes, dont l'employeur, à livrer des informations. Conformément aux principes de proportionnalité[142] et de finalité[143], *l'employeur doit, là encore, limiter la transmission des informations à celles qui relèvent de sa compétence* (salaires, attestations de périodes d'incapacité de travail, etc.)[144]. Il ne peut à notre sens pas transmettre toutes les informations en sa possession, mais uniquement celles qui sont en lien avec la période d'incapacité ou l'événement actuel. Le dossier constitué par le service des RH contenant toutes les informations relatives à la qualité prestation de travail (par exemple les évaluations annuelles) n'a ainsi pas à être transmis dans son intégralité. Quant aux informations médicales plus détaillées, elles n'ont ici pas à être transmises, d'autant moins que l'assureur dispose en principe des autorisations nécessaires pour se les procurer auprès des médecins du travailleur-assuré.

2. L'accès au dossier

En matière d'assurances sociales, le droit d'accéder au dossier est régi par l'art. 47 LPGA, qui ne mentionne pas l'employeur au rang des personnes ayant le droit de consulter le dossier constitué au sujet de l'assuré. Dans une affaire de 2005, le Tribunal fédéral a notamment justifié son refus de conférer à l'employeur la qualité pour s'opposer à une

---

140 Art. 31 al. 2 LPGA. Cf. KIESER, N 35 *ad* art. 31 LPGA.

141 Cf. la fiche explicative « Déclaration des accidents et des maladies professionnelles. Surveillance de l'évolution du cas. Paiement de l'indemnité journalière », établie par la Suva (réf. : 451.f), ch. 2.1.

142 Art. 4 al. 2 LPD.

143 Art. 4 al. 3 LPD.

144 Cf. note 132.

décision rendue par un assureur LAA (sur la question du droit à une rente d'invalide) par les problèmes que cela engendrerait sous l'angle de la protection des données.

Reconnaître à l'employeur la qualité pour former opposition équivalant à lui conférer le statut de partie à la procédure entraînerait automatiquement le droit pour ce dernier de prendre connaissance de l'intégralité du dossier[145]. Or, selon le Tribunal fédéral, « le dossier contient notoirement des données sensibles relatives à l'état de santé de l'assuré (rapports médicaux, expertises médicales). Même si, comme en l'espèce, le travailleur a pu, dans un premier temps, donner son accord à la consultation du dossier par son employeur, ses droits à la protection de la personnalité entreraient inévitablement en conflit avec les droits de partie de l'employeur au stade de la procédure probatoire »[146]. À l'issue de cette réflexion, notre Haute Cour s'interroge sur l'opportunité, toujours pour les raisons invoquées, tenant à la protection des données, de revenir sur une jurisprudence antérieure reconnaissant à l'employeur le droit de former opposition contre une décision déniant la qualité d'assuré au travailleur, ou niant la réalisation d'un accident[147]. La question a été laissée ouverte[148].

Dans certains cas, l'assureur et l'employeur peuvent être amenés à *collaborer, de manière plus ou moins formelle, dans l'intérêt de l'employé-assuré*. Dans ce cas, l'employeur peut être amené à accéder à certains éléments du dossier, notamment à certaines précisions concernant l'état de santé de l'assuré. Ainsi, dans le cadre de l'assurance-invalidité, certaines mesures d'intervention précoce[149], comme l'adaptation du poste de travail, supposent l'accord de l'employeur, ce qui suppose logiquement qu'il comprenne les raisons des aménagements qui lui sont demandés. Dans le cadre de l'assurance collective d'indemnités journalières en cas de maladie, de plus en plus d'assureurs recourent au *case management* lorsque l'incapacité de travail se prolonge. Parfois, on tente dans ce cadre de trouver une solution pour l'employé au sein de l'entreprise, ce qui suppose là encore la collaboration de l'employeur. On peut aussi songer aux mesures relatives au marché de l'emploi dans le cadre de l'assurance-chômage. Le succès de certaines mesures, comme les stages professionnels[150] ou l'allocation d'initiation au travail pour les assurés dont le placement est difficile[151], suppose à notre sens que les entreprises auprès desquelles ces mesures sont effectuées bénéficient d'informations suffisantes sur les particularités de la

145 Cf. art. 47 al. 1 let. b LPD.

146 ATF 131 V 298 c. 6.2. A noter que le Tribunal fédéral a également dénié à l'employeur le droit de s'opposer à une décision de l'assurance-invalidité (ATF 130 V 560). Dans cette affaire, la protection des données n'était toutefois pas un argument pour fonder sa position.

147 Cf. ATF 106 V 222 c. 1.

148 ATF 131 V 298 c. 6.2.

149 Cf. art. 7d LAI.

150 Cf. art. 64a al. 1 let. b LACI.

151 Cf. art. 65 LACI.

situation de la personne qu'elles accueillent. Il ne s'agit ici pas nécessairement d'informations d'ordre médical, mais, d'une manière plus générale, d'ordre socio-professionnel.

3. La transmission spontanée d'informations à l'employeur

L'instruction du dossier par l'assureur, social ou privé, peut l'amener à découvrir des faits dont l'employeur pourrait déduire des droits à l'encontre de son employé. On peut ainsi imaginer l'exemple d'un rapport établi par un détective privé qui apporterait la preuve, sans aucun doute possible, d'un comportement malhonnête de la part de l'assuré, comportement qui pourrait justifier un licenciement avec effet immédiat.

Pour l'assureur social, un tel état de fait reste circonscrit par les art. 33 LPGA et 19 LPD. Selon ces dispositions, la communication des données personnelles n'est possible que s'il existe une base légale dans une loi au sens formel, ou, à défaut, que si l'une des quatre hypothèses mentionnées à l'art. 19 al. 1 LPD est remplie. En l'espèce, il n'existe pas de base légale qui autorise l'assureur social à communiquer spontanément des données personnelles de l'assuré à l'employeur de celui-ci. Des quatre hypothèses mentionnées, seule la dernière nous paraît pouvoir apporter une réponse à la question évoquée ici[152] : l'employeur pourrait tenter de rendre vraisemblable « que la personne concernée ne refuse son accord ou ne s'oppose à la communication que dans le but de l'empêcher de se prévaloir de prétentions juridiques ou de faire valoir d'autres intérêts légitimes »[153]. Cela suppose toutefois que l'employeur ait été informé de l'existence des données qu'il entend consulter, information que l'assureur n'est à notre avis pas habilité à transmettre. Une « *fishing expedition* » de la part de l'employeur n'est pas admissible sous l'angle de l'art. 19 al. 1 let. d LPD[154].

Vis-à-vis de l'assureur privé, cette question s'inscrit dans le cadre de la pondération des intérêts commandée par les art. 28 al. 2 CC et 13 al. 1 LPD. Pour que la transmission des données à l'employeur soit licite, il faudrait qu'elle soit justifiée par l'intérêt prépondérant de ce dernier[155]. L'hypothèse que nous visons ici ne figure pas dans la liste exemplative de

---

152 Il est en effet peu probable, dans une telle situation, que l'employé-assuré consente à la transmission des données (cf. art. 19 al. 1 let. b LPD).

153 Art. 19 al. 1 let. d LPD.

154 A titre de comparaison, l'art. 20 al. 1 LPD permet à la personne concernée qui rend vraisemblable un intérêt légitime de s'opposer à ce que l'organe fédéral responsable communique des données personnelles déterminées. Elle doit alors désigner précisément les données qu'elle entend soustraire à la communication, une opposition générale n'étant pas recevable (cf. MUND, N 4 *ad* art. 20 LPD).

155 L'intérêt privé pouvant justifier une atteinte à la personnalité n'est pas nécessairement l'intérêt de celui qui traite les données ou de celui que ces dernières concernent, mais peut également être l'intérêt d'un tiers (cf. WERMELINGER, N 11 *ad* art. 13 LPD).

l'art. 13 al. 2 LPD. À notre sens, seuls des faits gravissimes mettant en péril la sécurité de l'entreprise et/ou des collaborateurs[156], à la rigueur une atteinte très importante aux intérêts économiques de l'employeur, peut être à même de justifier la communication spontanée de données par l'assureur. Le simple fait que l'employeur aurait des droits en raison des faits révélés par l'instruction du cas, par exemple le droit de licencier le travailleur avec effet immédiat, ne devrait pas être suffisant.

Il est intéressant de noter qu'en l'état actuel du droit, l'assureur social ne peut en principe pas communiquer des informations à l'employeur pour des raisons majeures de sécurité de ce dernier ou de ses employés. L'avant-projet de loi révisée sur la protection des données, en consultation jusqu'au début du mois d'avril 2017, prévoit une exception à l'interdiction de communiquer les données lorsque « le traitement est nécessaire pour protéger la vie ou l'intégrité corporelle de la personne concernée ou d'un tiers », à condition qu'il ne soit pas possible d'obtenir le consentement de la personne concernée dans un délai raisonnable[157].

IV. Conclusion

Les questions traitées dans le cadre de cette contribution révèlent l'aspect tentaculaire du thème de la protection des données confiées aux assureurs, y compris dans le cadre plus restreint des rapports de travail et de la triangulation entre assuré, assureur et employeur. Nous n'avons pas la prétention d'avoir envisagé tous les problèmes pouvant se présenter en pratique et donner du fil à retordre aux défenseurs des trois parties impliquées.

Nous avons pu voir, dans la première partie de cette contribution, que l'assuré est finalement pratiquement transparent pour l'assureur qui, social ou privé, ne rencontre qu'une faible résistance lorsqu'il veut obtenir des informations, la réalité économique de l'assuré étant une arme parfaitement efficace à cet égard.

Nous avons vu également que les informations récoltées par un assureur, soit-il social, soit-il privé, sont facilement accessibles aux autres assureurs et à certaines autorités

156 Par exemple, les rapports médicaux révéleraient que l'employé est atteint d'une maladie grave, potentiellement épidémique (par exemple Ebola), ou l'enquête réalisée par un détective privé montrerait la volonté de l'assuré de s'en prendre physiquement à l'employeur ou aux collaborateurs de l'entreprise.

157 Art. 27 al. 3 let. c AP-LPD. Cet ajout correspond à l'art. 10 let. b de la directive (UE) 2016/680 et à l'art. 6 par. 1 let. d du règlement (UE) 206/679 (cf. rapport explicatif du 21 décembre 2016 concernant l'avant-projet de loi fédérale sur la révision totale de la loi sur la protection des données et sur la modification d'autres lois fédérales, p. 68).

administratives. Le nombre d'organes et de personnes susceptibles de prendre connaissance de données personnelles a priori protégées est exponentiel.

L'employeur semble quelque peu en retrait de ce circuit d'information : n'étant pas une autorité administrative, il ne bénéficie pas de l'assistance que les assureurs sociaux et certaines autres administrations se doivent mutuellement. En lui refusant la qualité de partie dans une affaire précisément pour des motifs tenant à la protection des données, le Tribunal fédéral a clairement manifesté sa volonté de le maintenir à l'extérieur des flux d'information s'échangeant entre assureurs sociaux. Dans le domaine de l'assurance privée, il ne doit pas avoir un accès automatique aux données de l'assureur. Compte tenu de la transparence des flux d'information en amont, cette rigueur est indispensable.

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.

BAERISWYL BRUNO, Commentaire de l'art. 4 LPD, *in* : Bruno Baeriswyl/Kurt Pärli (éds.), Datenschutzgesetz (DSG) - Handkommentar, Berne 2015.

CARUZZO PHILIPPE, Le contrat individuel de travail – Commentaire des articles 319 à 321 du Code des obligations, Zurich/Bâle/Genève 2009.

CHAPPUIS BENOÎT, Les moyens de preuve collectés de façon illicite ou produits de façon irrégulière, *in* : Franz Werro/Pascal Pichonnaz (éds.), Le procès en responsabilité civile, Berne 2011, pp. 108-174.

DUPONT ANNE-SYLVIE, Le droit de réplique en assurances sociales, *in* : François Bohnet (éd.), Le droit de réplique, Neuchâtel 2013, pp. 83-149.

FUHRER STEPHAN, Schweizerisches Privatversicherungsrecht, Zurich/Bâle/Genève 2011.

GUILLOD OLIVIER, Le cadre juridique de la transmission de données personnelles aux assureurs, *in* : Olivier Guillod (éd.), Protection des données médicales et transparence… du patient ? 19e Journée de droit de la santé, Neuchâtel 2012, pp. 135-144.

KIESER UELI, ATSG Kommentar, 3e édition, Zurich 2015.

MANAÏ DOMINIQUE, Droits du patient face à la biomédecine, Berne 2013.

MONTAVON MICHEL, Communications de données médicales sur le patient entre prestataires de soins et assureur-maladie – Ménage à trois, *in* : RFJ 2015, pp. 235-257.

MOSER-SZELESS MARGIT, La surveillance comme moyen de preuve en assurance sociale, *in* : RSAS 2013, pp. 129-156.

MUND CLAUDIA, Commentaire de l'art. 20 LPD, *in* : Bruno Baeriswyl/Kurt Pärli (éds.), Datenschutzgesetz (DSG) - Handkommentar, Berne 2015.

PÄRLI KURT, IIZ-Datenaustausch. Datenschutz und Datenaustausch in der Interinstitutionnellen Zusammenarbeit (IIZ), Zurich/Bâle/Genève 2014 (cité : PÄRLI, *IIZ*).

PÄRLI KURT, Datenaustausch zwischen Arbeitgeber und Versicherung. Problematische Bearbeitung von Arbeitnehmergesundheitsdaten bei der Begründung der privatwirtschaftlichen Arbeitsverhältnisses, *in* : REAS I/2004, pp. 32-37 (cité : PÄRLI, *REAS*).

PRIEUR YVONNE, Datenschutz im Sozialversicherungswesen, *in* : Nicolas Passadelis/David Rosenthal/Hanspeter Thür (éds.), Datenschutzrecht, Bâle 2015, pp. 431-485.

VALTERIO MICHEL, Droit de l'assurance-vieillesse et survivants (AVS) et de l'assurance-invalidité (AI), Zurich 2011.

WERMELINGER AMÉDÉO, Commentaire de l'art. 13, *in* : Bruno Baeriswyl/Kurt Pärli (éds.), Datenschutzgesetz (DSG) - Handkommentar, Berne 2015.

ZITTEL NIGGI, Datenschutz in der Privatversicherung, *in* : Nicolas Passadelis/David Rosenthal/ Hanspeter Thür (éds.), Datenschutzrecht, Bâle 2015, pp. 407-429.

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].

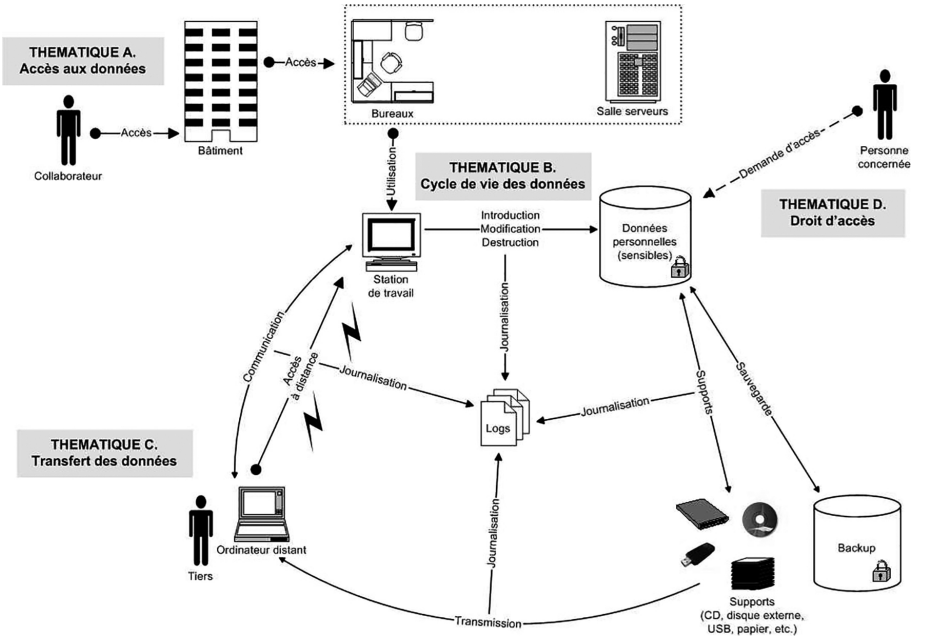
Il est organisé en quatre thématiques : l'accès aux données, le cycle de vie des données, le transfert des données et le droit d'accès aux données. Pour chaque thématique, différents points auxquels il faut veiller sont mis en exergue. Des mesures sont proposées y relativement, mesures qui constituent 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 (OPrI, 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.

KARINE LEMPEN*

Protection des données et discrimination lors de la procédure de recrutement

Sommaire

		Page
I.	Introduction	270
II.	Trois régimes complémentaires	271
	A. Protection contre les discriminations	271
	B. Protection des données	272
	C. Protection de la personnalité dans le cadre des relations de travail	273
	D. Convergences	274
	1. Données sensibles (art. 3 LPD), critères prohibés (art. 8 Cst.)	274
	2. Principes généraux : la portée du consentement	276
	3. Lois contemporaines, en cours de révision (LPD, LEg)	278
III.	Questions choisies	279
	A. Curriculum vitae	279
	B. Entretien d'embauche	280
	C. Recherche de données sur Internet	282
	1. Généralités	282
	2. Réseaux sociaux	282
	3. Moteurs de recherche	283
IV.	Conclusion	284
Bibliographie		285

* Je remercie Mme Elsa Perdaems, assistante à la Faculté de droit de l'Université de Genève, d'avoir contribué à la préparation de cet article.

I. Introduction

Le traitement de données personnelles lors d'une procédure de recrutement peut porter atteinte à la personnalité et présente, de surcroît, « un risque de discrimination »[1] pour la personne candidate.

En Suisse, lorsque le traitement des données à l'embauche entraîne non seulement une atteinte illicite à la personnalité, mais aussi une discrimination, la personne concernée peut se prévaloir simultanément de différents droits, en particulier:

- le droit fondamental à ne pas être discriminé (art. 8 al. 2 Cst.), concrétisé par deux lois fédérales sur l'égalité[2];
- le droit fondamental à la protection de la sphère privée (art. 13 Cst.), que la loi fédérale sur la protection des données (LPD) contribue à réaliser entre particuliers[3];
- le droit à ne pas subir d'atteinte illicite à la personnalité dans le cadre des rapports de travail (art. 328 et 328b CO).

Alors que les rapports entre les normes de droit du travail protégeant la personnalité et la loi sur la protection des données suscitent de nombreux commentaires[4], rares sont les écrits qui examinent la façon dont les deux derniers régimes (328b CO et LPD) s'articulent avec le premier (art. 8 al. 2 Cst.)[5].

La présente contribution explore la manière dont le droit antidiscriminatoire interagit avec les normes de protection des données et de la personnalité dans le cadre d'une procédure d'embauche. L'accent est mis sur le traitement des données par des personnes ou entités privées.

La partie qui suit présente brièvement les trois régimes en question et met en évidence leur complémentarité. Dans un second temps, nous analyserons à la lumière des différentes normes protectrices trois questions afférentes à la procédure de sélection du personnel.

---

1 Voir l'art. 6 par. 2 du projet de Convention du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (P-STE-108), texte consolidé, septembre 2016.

2 Voir *infra* partie II, lettre A.

3 Message LPD, FF 2003 1915, 1962.

4 Notamment : AUBERT, pp. 148 ss ; STREIFF/VON KAENEL/RUDOLPH, N 3 *ad* art. 328b CO ; DUNAND, N 4 *ad* art. 328b CO.

5 Parmi ces écrits, voir, en particulier, l'article rédigé par LE MÉTAYER/LE CLAINCHE à propos du droit français.

II. Trois régimes complémentaires

A. Protection contre les discriminations

La Constitution fédérale interdit la discrimination fondée sur l'origine, la race, le sexe, l'âge, la langue, la situation sociale, le mode de vie, les convictions ou le handicap (art. 8 al. 2 Cst.). La liste est exemplative. L'identité de genre et l'orientation sexuelle font aussi partie des critères « sensibles »[6].

Dans le domaine du travail, ce principe de non-discrimination est concrétisé par deux lois fédérales : la Loi du 24 mars 1995 sur l'égalité entre femmes et hommes (LEg) et la Loi du 13 décembre 2002 sur l'égalité pour les handicapés (LHand). La première s'applique à l'ensemble des rapports salariés de droit privé ou public. La seconde, en revanche, ne vise que les rapports de travail régis par la Loi sur le personnel de la Confédération (LPers).

En sa qualité d'employeuse, « la Confédération utilise tous les moyens dont elle dispose pour assurer des chances égales aux personnes handicapées. Elle prend les mesures propres à mettre en œuvre la [LHand] dans les rapports de travail à tous les échelons, en particulier lors de l'engagement de son personnel » (art. 13 LHand)[7]. « La personne handicapée qui a des raisons de penser que sa candidature n'a pas été retenue à cause de son handicap peut exiger de l'employeur qu'il indique par écrit les motifs pour lesquels la candidature a été écartée » (art. 14 OHand). Toutefois, un refus d'embauche discriminatoire fondé le handicap ne donne droit à aucune indemnité spécifique[8].

La Loi sur l'égalité entre femmes et hommes interdit de discriminer une personne à l'embauche sur la base de son sexe en se fondant, notamment, sur son état civil, sa situation familiale ou sa grossesse (art. 3 al. 1 et 2 LEg). La loi réserve la possibilité, pour les responsables du recrutement, de se référer au critère du sexe (en adoptant des quotas, par exemple), pour autant que les mesures soient « appropriées » (proportionnalité) et visent « à promouvoir dans les faits l'égalité entre femmes et hommes » (finalité) (art. 3 al. 3 LEg)[9]. « La personne qui n'est pas engagée et qui se prévaut d'une discrimination peut exiger de l'employeur qu'il motive sa décision par écrit » (art. 8 al. 1 LEg). Contrairement à ce qui a été indiqué plus haut en lien avec le handicap, une décision de non-embauche

---

6 WALDMANN, pp. 625-627, 715 s.

7 Voir aussi l'art. 4 al. 2 let. f LPers.

8 Voir à ce sujet SCHEFER/HESS-KLEIN, pp. 95-97, selon lesquels le « droit à une motivation écrite du refus d'engagement, fondé sur l'art. 14 OHand, demeure donc sans effet » (p. 96).

9 Au sujet des mesures positives dans le domaine de l'emploi, voir LEMPEN, N 38-49 *ad* art. 3 LEg. Sur la licéité des quotas rigides dans le secteur public, voir l'ATF 131 II 361, c. 5-7.

basée sur le sexe donne droit à une indemnité spéciale (art. 5 al. 2 LEg)[10], dont le montant n'excédera cependant pas une somme équivalente à trois mois de salaire (art. 5 al. 4 LEg).

B. Protection des données

Aux termes de la Constitution fédérale, « toute personne a le droit d'être protégée contre l'emploi abusif des données qui la concernent » (art. 13 al. 2 Cst.). La Loi fédérale sur la protection des données « vise à protéger la personnalité et les droits fondamentaux des personnes qui font l'objet d'un traitement de données » (art. 1 LPD). La loi régit notamment le traitement de données personnelles[11] par des personnes privées (art. 2 al. 1 let. a LPD).

Les données personnelles dont le traitement risque particulièrement de porter atteinte à la personnalité sont qualifiées de « sensibles »[12]. Sont notamment « sensibles », les données relatives aux « opinions ou activités religieuses, philosophiques, politiques ou syndicales » ainsi que celles concernant « la santé, la sphère intime ou l'appartenance à une race » (art. 3 let. c ch. 1-2). Nous y reviendrons plus loin[13].

La loi sur la protection des données énonce un certain nombre de principes généraux[14]. Tout traitement de données doit être licite (art. 4 al. 1 LPD), conforme à la bonne foi et proportionné (art. 4 al. 2 LPD). Les données personnelles doivent être collectées dans un but déterminé (art. 4 al. 3 LPD), reconnaissable pour la personne concernée (art. 4 al. 4 LPD). La personne qui traite les données doit s'assurer de leur « exactitude » (art. 5 al. 1 LPD) et prendre les mesures de « sécurité » appropriées (art. 7 al. 1 LPD).

Le traitement de données « sensibles » requiert le « consentement » libre, éclairé et « explicite » de la personne concernée[15]. Un consentement exprès[16] de cette dernière est aussi nécessaire pour établir un « profil de la personnalité » (art. 4 al. 5 LPD).

Un récent avant-projet[17] de loi révisée sur la protection des données propose de remplacer la notion de « profil de la personnalité » par celle, dynamique[18], de « profilage ». Ce terme

---

10 ATF 131 II 361, c. 4.

11 Qui « se rapportent à une personne identifiée ou identifiable » (art. 3 let. a LPD).

12 MEIER, N 469.

13 Partie II, lettre D, chiffre 1.

14 Pour un exposé détaillé de ces principes, voir MEIER, N 637 ss.

15 DUNAND, N 16 *ad* art. 328b CO.

16 Sur le consentement « exprès », voir l'art. 4 al. 6 AP-LPD et le rapport explicatif, p. 46.

17 Au sujet de cet avant-projet mis en consultation le 21 décembre 2016, voir la contribution de CAMILLE DUBOIS dans cet ouvrage, pp. 47 ss.

18 Rapport explicatif, p. 43.

désigne « toute exploitation de données personnelles ou non, consistant à analyser ou à prédire les caractéristiques essentielles d'une personne, notamment son rendement au travail, sa situation économique, sa santé, sa sphère intime, ou ses déplacements »[19]. L'analyse de ces caractéristiques peut avoir pour but de déterminer si une personne est apte à exercer une certaine activité. Les données issues d'un profilage sont, en principe, des données personnelles, parfois sensibles[20].

La loi sur la protection des données pose le principe selon lequel le traitement de données personnelles par des personnes privées « ne doit pas porter une atteinte illicite à la personnalité des personnes concernées » (art. 12 al. 1 LPD). La loi mentionne différentes situations où une atteinte à la personnalité est présumée (art. 12 al. 2 LPD). Une telle atteinte « est illicite à moins d'être justifiée par le consentement de la victime, par un intérêt prépondérant privé ou public, ou par la loi » (art. 13 al. 1 LPD). Un intérêt prépondérant privé peut être retenu si le traitement des données « est en relation directe avec la conclusion » d'un contrat de travail et les données concernent la personne candidate (art. 13 al. 2 let. a LPD).

C. Protection de la personnalité dans le cadre des relations de travail

L'article 328b CO règle spécifiquement le traitement de données personnelles lors du recrutement[21] et durant les rapports de travail de droit privé[22].

Adopté simultanément à la loi fédérale sur la protection des données, l'article 328b CO renforce la protection de la personnalité dans le cadre des rapports de travail[23] en autorisant le traitement de données dans deux cas seulement[24]:

– avant la conclusion du contrat de travail et durant son exécution, lorsque les « données portent sur les aptitudes du travailleur à remplir son emploi » (art. 328b al 1 CO) ;

---

19 Art. 3 let. f AP-LPD.

20 Rapport explicatif, p. 43.

21 Voir TF, 2C_103/2008 du 30 juin 2008, auquel se réfèrent notamment STREIFF/VON KAENEL/RUDOLPH, N 4 *ad* art. 328b CO ; DUNAND, N 5 *ad* art. 328b CO et PÄRLI, N 6 *ad* art. 328b CO. Voir aussi AUBERT, N 2 *ad* art. 328b CO.

22 PÄRLI, N 4 *ad* art. 328b CO précise que les rapports de travail avec la Confédération sont soumis à la LPD, mais n'entrent pas dans le champ d'application de l'art. 328b CO.

23 PÄRLI, N 1 *ad* art. 328b CO.

24 Selon son texte, l'art. 328b CO « délimite plus étroitement » que les art. 12 et 13 LPD les informations que l'employeur est autorisé à traiter (AUBERT, N 1 *ad* art. 328b CO). Voir aussi : STREIFF/VON KAENEL/RUDOLPH, N 3 *ad* art. 328b CO ; PÄRLI, N 5 *ad* art. 328b CO.

– durant les rapports de travail, lorsque les données « sont nécessaires à l'exécution du contrat de travail » (art. 328b al. 1 CO)[25].

Dans ces deux hypothèses uniquement, le traitement des données personnelles par une personne ou entité employeuse est présumé licite. La preuve du non-respect des principes généraux du droit – notamment la bonne foi et la proportionnalité – permet de renverser cette présomption de licéité[26].

En effet, même dans les deux situations susmentionnées, le traitement de données doit respecter les principes prévus par la loi sur la protection des données[27], à laquelle renvoie l'article 328b CO *in fine*.

Comme nous le verrons plus loin à propos des renseignements pris sur Internet[28], l'application de ces principes signifie, notamment, que le traitement des données ne doit pas se faire à l'insu de la personne candidate et « que l'employeur ne doit traiter que les données strictement nécessaires, et de la manière la moins intrusive possible »[29].

D. Convergences

1. Données sensibles (art. 3 LPD), critères prohibés (art. 8 Cst.)

Les trois régimes exposés poursuivent des objectifs similaires et visent en partie les mêmes catégories[30]. Les critères prohibés énumérés à l'article 8 alinéa 2 Cst. et les données sensibles mentionnées par l'article 3 lettre c LPD sont particulièrement susceptibles de porter atteinte à la personnalité[31].

L'avant-projet susmentionné prévoit d'inclure dans la liste exhaustive figurant à l'article 3 lettre c LPD deux nouveaux types de données sensibles : les « données génétiques »[32] et

---

25 PFPDT, Guide, p. 6.

26 AUBERT, p. 150 ; ATF 130 II 425, c. 3.3.

27 MEIER, N 2055 ; DUNAND, N 34 *ad* art. 328b CO. Voir les ATF 136 II 508, c. 5.2.4 ; 138 II 346, c. 7.2. (la justification d'un traitement de données contrevenant aux principes généraux ne peut être admise dans un cas d'espèce qu'avec une grande retenue).

28 Partie III, lettre C.

29 DUNAND, N 36-37 *ad* art. 328b CO, avec les références.

30 LE MÉTAYER/LE CLAINCHE arrivent au même constat à propos du droit français.

31 PÄRLI, p 129. Voir aussi MEIER, N 469, à propos des données listées à l'art. 3 let. c LPD.

32 La Loi fédérale du 8 octobre 2004 sur l'analyse génétique humaine interdit de discriminer sur la base du patrimoine génétique (RS 810.12) (art. 4 LAGH). Lors du recrutement, les tests génétiques sont en principe interdits (art. 21 LAGH). Des exceptions sont prévues pour les analyses génétiques présymptomatiques visant à prévenir les maladies professionnelles et les accidents (art. 22 ss LAGH). L'avant-projet de LAGH révisée ne prévoit aucune modification à ce sujet. Selon le rapport explicatif

« les données biométriques qui identifient un individu de façon unique »[33]. En revanche, il n'est pas prévu d'ajouter la mention du « handicap », puisque ce critère – prohibé par l'art. 8 al. 2 Cst. – peut être rattaché à celui de la « santé »[34].

L'« orientation sexuelle », qui ne figure explicitement ni sur la liste des motifs prohibés (art. 8 al. 2 Cst.), ni sur celle des données sensibles (art. 3 let. c LPD), est en réalité couverte par les deux dispositions. En effet, comme évoqué plus haut[35], la protection offerte par l'art. 8 al. 2 Cst. ne se limite pas aux motifs énumérés par cette disposition et s'étend à l'orientation sexuelle. En outre, les informations à ce sujet ont trait à la « vie sexuelle » et font dès lors partie des données relatives à la « sphère intime » au sens de l'article 3 lettre c chiffre 2 LPD[36]. À cet égard, il est intéressant de relever que le nouveau droit de l'Union européenne interdit, en principe, le traitement de données « concernant la vie sexuelle ou l'orientation sexuelle »[37].

Absent des catalogues de données nécessitant une protection particulière au niveau suisse et européen[38], le critère du « sexe », contrairement à celui de l'orientation sexuelle, semble à première vue ne pouvoir être rattaché à aucune des catégories sensibles prévues par le droit de la protection des données.

En revanche, sous l'angle de l'article 8 Cst., le sexe figure parmi les motifs principaux de discrimination et le fait que ce critère ne soit pas défini comme une donnée sensible par l'article 3 LPD surprend.

Une telle absence peut certes s'expliquer par le fait que cette disposition vise des « informations confidentielles qu'il convient de traiter avec discrétion accrue »[39]. Or, le sexe d'une personne est rarement confidentiel. Dans le cadre de l'art. 328b CO, ce critère

---

du 18 février 2015, « on ne recourt pas encore, dans le domaine du travail, aux analyses génétiques […] dans le cadre d'un examen médical d'embauche. […] la plupart des prédispositions pouvant être plus ou moins d'origine génétique sont établies actuellement par un diagnostic clinique traditionnel ». Toutefois, « il y a lieu de garder à l'esprit que le progrès continu des méthodes diagnostiques génétiques pourrait amener une modification relativement rapide de la situation » (pp. 84-85).

33 Voir l'art. 3 let. c ch. 3-4 AP-LPD.

34 Mentionné à l'art. 3 let. c ch. 2 LPD.

35 Voir *supra* partie II, lettre A.

36 Rapport explicatif, p. 42.

37 Voir le règlement (UE) 2016/679 du 27 avril 2016, art. 9 par. 1.

38 Le critère du sexe ne figure ni à l'art. 3 let. c LPD, ni à l'art. 9 du règlement (UE) 2016/679 du 27 avril 2016. Il n'est pas non plus mentionné à l'art. 6 de la Convention du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel du 28 janvier 1981 (STE 108). L'art. 6 P-STE 108 ne se réfère pas davantage au sexe. Au sujet de cette convention et de la révision en cours, voir DUBOIS dans le présent ouvrage.

39 DUNAND, N 15 *ad* art. 328b CO, qui se réfère à AUBERT, p. 147.

est considéré comme une donnée personnelle qui, au même titre que l'adresse ou le numéro d'AVS, permet d'identifier une personne – notamment lors d'un recrutement – et dont le traitement ne pose en général pas problème[40].

Toutefois, la « race »[41], expressément citée en droit suisse et européen parmi les données sensibles[42], confidentielles, peut être facilement reconnaissable dès la première rencontre physique. Il en va de même du handicap, rattaché à la catégorie « santé », qui peut parfois être tout aussi visible que le sexe biologique d'une personne.

En outre, le sexe biologique peut (devoir) être dissimulé. *Transgender Network Switzerland* donne le conseil suivant : « Vous n'êtes pas obligé_e de signaler que vous êtes trans* dans une candidature, à moins qu'il ne s'agisse d'une information pertinente pour le poste envisagé. Si vous n'avez pas encore changé de (pré)nom et d'état civil, vous êtes toutefois obligé_e de les mentionner au plus tard lorsque vous avez obtenu le poste »[43].

Un cas zurichois concernant une candidate évincée parce qu'elle avait raconté avoir effectué, par le passé, une opération de changement de sexe, illustre les risques inhérents à la révélation de ce type d'informations dans le cadre d'une procédure d'embauche. En l'espèce, l'autorité de conciliation a qualifié le refus d'embauche de discriminatoire au sens de l'article 3 LEg et les parties se sont mises d'accord sur une indemnité correspondant à deux mois de salaire[44].

Au regard de l'interdiction de discriminer en raison du sexe prévue par l'article 3 LEg et des discriminations vécues par les personnes trans* dans le domaine de l'emploi, il convient de garder à l'esprit que les données sur le sexe d'une personne peuvent parfois – à l'instar de celles sur l'orientation sexuelle – relever de la « sphère intime » et être, dès lors, « sensibles ».

2. Principes généraux : la portée du consentement

Les régimes juridiques de lutte contre la discrimination et de protection des données ou de la personnalité reposent de façon similaire sur les principes de proportionnalité et de finalité[45]. En revanche, la place accordée au consentement varie.

---

40 RUDOLPH, pp. 48 s. L'auteur (note 60) se demande toutefois si les questions relatives au sexe d'une personne sont encore admissibles depuis l'entrée en vigueur de la LEg.

41 L'art. 3 let. c ch. 2 AP-LPD remplace « la race » par « l'origine raciale ou ethnique ».

42 Voir les dispositions citées à la note 38.

43 https://www.transgender-network.ch/ > Consultations > Droit > Informations juridiques > 8. Monde du travail (consulté le 29.12.2016).

44 Voir le résumé de cette affaire sur : www.gleichstellungsgesetz.ch, ZH/165 (2008).

45 A titre d'illustration, voir l'art. 4 al. 2 et 3 LPD et l'art. 3 al. 3 LEg.

En effet, au regard des inégalités de pouvoir existant entre les groupes sociaux, le droit antidiscriminatoire s'intéresse peu à un éventuel consentement de la victime, rarement « libre »[46]. Le droit relatif à la protection de la personnalité, en revanche, mentionne le consentement parmi les motifs susceptibles de lever l'illicéité d'un comportement (art. 28 al. 2 CC, 13 al. 1 LPD).

En réalité, cette différence entre les régimes est moins importante qu'il n'y paraît au premier abord. En effet, la loi sur la protection des données précise qu'une personne « ne consent valablement que si elle exprime sa volonté librement et après avoir été dûment informée. Lorsqu'il s'agit de données sensibles et de profils de la personnalité, son consentement doit au surplus être explicite » (art. 4 al. 5 LPD)[47].

Le Conseil fédéral explique qu'un « travailleur contraint de donner son consentement, sous la menace d'un licenciement, à un traitement de données qui n'est pas nécessaire à l'exécution du contrat de travail n'est pas en mesure de donner son consentement librement »[48]. Eu égard au rapport de subordination inhérent au contrat de travail, l'existence d'un consentement libre et éclairé doit être admise avec une grande prudence dans le contexte professionnel[49] et notamment dans le cadre d'une procédure d'embauche.

En outre, vu la nature relativement impérative de l'article 328b CO[50], une personne candidate ne pourra consentir valablement au traitement de données sans rapport avec ses aptitudes professionnelles que si la dérogation est dans son propre intérêt[51].

Par exemple, une personne postulant auprès d'une entreprise soucieuse d'encourager les candidatures des chômeurs et chômeuses en situation de handicap peut avoir intérêt à révéler des informations relatives à une maladie sans effet sur son aptitude au travail. Nous reviendrons sur cette hypothèse dans la section consacrée au curriculum vitae[52].

---

46 Voir EMMENEGGER, pp. 174-176, à propos du harcèlement sexuel dans les relations de travail. L'auteure montre qu'une conception orientée vers la protection de la personnalité se focalise sur le « consentement » et méconnaît les rapports de pouvoir existants.

47 Au sujet de la nouvelle terminologie proposée pour cette disposition, voir l'art. 4 al. 6 AP-LPD et *supra* Partie II, lettre B.

48 Message LPD, FF 2003 1915 (1940). Dans le même sens : règlement (UE) 2016/679 du 27 avril 2016, art. 7 par. 4.

49 MEIER, N 2057 ; PÄRLI, N 20 *ad* art. 328b CO.

50 Mentionné à l'art. 362 CO.

51 Voir, notamment, DUNAND, N 32 *ad* art. 328b CO ; PORTMANN/RUDOLPH, N 26 *ad* art. 328b CO ; PÄRLI, N 8 *ad* art. 328b CO, avec les références.

52 Partie III, lettre A.

3. Lois contemporaines, en cours de révision (LPD, LEg)

Les lois fédérales sur la protection des données (LPD) et sur l'égalité entre femmes et hommes (LEg)[53] datent de la première moitié des années nonante. Toutes deux sont construites selon le même schéma : une partie générale, une partie consacrée au droit privé puis une partie relative au droit public. Le fait que ces lois traitent d'un même problème « parallèlement »[54] en droit public et en droit privé rend leur maîtrise difficile – eu égard aux spécificités propres à chaque régime – et ne favorise probablement pas le recours à ces instruments juridiques en justice.

Une violation de la LPD ou de la LEg peut donner lieu aux actions prévues à l'article 28a CC, mentionnées par les articles 15 LPD[55] et 5 alinéa 1 LEg. Lorsque le traitement des données à l'embauche entraîne non seulement une atteinte illicite à la personnalité, mais aussi une discrimination fondée sur le sexe, la personne candidate peut prétendre, sur la base de l'article 5 alinéas 2 et 4, LEg, à une indemnité correspondant au maximum à trois mois du salaire auquel la personne aurait vraisemblablement eu droit[56]. Elle peut en outre faire valoir ses droits à des dommages-intérêts (art. 41 ss CO) et à la réparation d'un tort moral (art. 49 CO), expressément réservés par les articles 28a alinéa 3 CC et 5 alinéa 5 LEg[57].

La LPD et la LEg prévoient ainsi des remèdes similaires, la seconde donnant droit à une indemnité supplémentaire en cas de refus d'embauche discriminatoire. En pratique, toutefois, la protection reste peu efficace dans le contexte d'une procédure d'embauche, notamment en raison des difficultés liées à la preuve de l'atteinte[58].

Actuellement, ces lois font l'objet d'une révision dans le but, notamment, d'améliorer la transparence – salariale en ce qui concerne la LEg – et de renforcer les contrôles[59]. Dans les deux cas, il s'agit de faciliter l'accès à la justice des individus concernés. L'avant-projet de loi révisée sur la protection des données propose notamment de supprimer les frais de justice pour les actions civiles en matière de protection des données[60]. La gratuité de la

---

53 Voir *supra* Partie II, lettre A.

54 Voir AUBERT, préface, p. X.

55 Sur les voies de droit prévues par la LPD, voir la contribution d'AURÉLIEN WITZIG dans le présent volume, pp. 25 ss.

56 Voir aussi *supra* Partie II, lettre A.

57 Voir RUDOLPH, pp. 112-118.

58 Pour plus d'explications : STREIFF/VON KAENEL/RUDOLPH, N 19 *ad* art. 328b CO, avec les références. Voir en particulier RUDOLPH, pp. 117 s.

59 Au sujet de la révision de la LPD, nous renvoyons à la contribution de CAMILLE DUBOIS dans ce volume. Concernant la LEg, voir le communiqué « Une avancée vers l'égalité salariale : le Conseil fédéral veut un message d'ici à l'été 2017 » publié par le Conseil fédéral le 26 octobre 2016.

60 Rapport explicatif, p. 86.

procédure est déjà prévue pour les procédures cantonales fondées sur la LEg (art. 114 let. a CPC). Dans la plupart des cantons, la partie qui succombe doit néanmoins verser des dépens qui peuvent s'élever, suivant les cas, à plusieurs milliers de francs.

III. Questions choisies

A. Curriculum vitae

Le curriculum vitae (CV) anonyme est parfois conçu comme un moyen de concilier, dès le début de la procédure d'embauche, les impératifs de protection des données et de lutte contre les discriminations[61].

En général, cette mesure consiste à supprimer du dossier de candidature le nom, le prénom, l'adresse, la nationalité, l'âge, le genre, la situation familiale et la photographie de la personne postulante[62]. Les responsables du recrutement sont ainsi amenés à ne traiter que des informations liées aux « aptitudes du travailleur à remplir son emploi » (art. 328b CO) et risquent moins de discriminer, volontairement ou non, sur la base de caractéristiques protégées par l'art. 8 al. 2 Cst.

Toutefois, comme évoqué plus haut en lien avec la possibilité d'autoriser une dérogation à la règle, relativement impérative, prévue à l'article 328b CO, une personne candidate peut avoir intérêt à communiquer des données personnelles sensibles (art. 3 let. c LPD) sans rapport avec son aptitude à exercer un emploi[63]. Par exemple, une personne qui souffre d'un handicap non visible au premier abord et actuellement sans conséquence sur sa capacité à travailler peut avoir intérêt à le mentionner dans son dossier, afin de rendre visibles les raisons pour lesquelles elle a eu besoin de plus de temps pour achever ses études ou alors parce que l'offre d'emploi encourage expressément les candidatures des personnes handicapées[64].

Au regard des efforts fournis actuellement en Suisse pour mieux utiliser le potentiel de la main d'œuvre indigène[65], on peut s'attendre à ce qu'un nombre croissant d'entreprises adopte des mesures positives visant à favoriser l'engagement de personnes qualifiées, en

---

61 Voir WERMELINGER, p. 1449.

62 SCHÖNENBERGER/FIBBI, p. 29. Au sujet des expériences faites en Suisse à l'étranger, notamment en France et en Allemagne, voir SCHÖNENBERGER/FIBBI, pp. 31 s.

63 Voir *supra* partie II, lettre D, chiffre 2.

64 Voir OFPER, pp. 4 s.

65 Voir le site www.personnelqualifie-suisse.ch/fr/ lancé en mai 2016 par la Confédération, les cantons et les partenaires sociaux.

particulier des seniors et des femmes. Le cas échéant, ces personnes auront tout intérêt à mentionner sur leur CV leur date de naissance et leur sexe.

Sachant que l'administration fédérale préconise de prendre en considération les expériences extra-professionnelles pour « évaluer si des qualifications sont équivalentes » lors de la sélection du personnel[66], une personne candidate avec des responsabilités familiales aura avantage à faire figurer cette information dans son curriculum vitae.

Enfin, si l'origine raciale ou ethnique fait partie des motifs de discrimination mentionnés par l'art. 8 al. 2 Cst. et que les données y relatives sont qualifiées de sensibles par l'art. 3 let. c ch. 2 LPD, il n'en demeure pas moins qu'une personne avec une couleur de peau foncée ou portant un voile peut, hélas, dans une société encore souvent raciste, préférer assortir son CV d'une photographie afin de s'épargner une rencontre avec un employeur hostile[67].

B. Entretien d'embauche

En vertu de l'art. 328b CO, les personnes qui mènent un entretien d'embauche ont le droit de poser uniquement des questions permettant de déterminer l'aptitude de la personne candidate à exercer l'emploi convoité[68].

Sont a priori interdites les questions sans rapport avec l'activité à exercer et portant atteinte à la sphère privée[69], telles que celles relatives à l'orientation sexuelle[70] ou à l'origine ethnique. Une question relative à l'origine de la personne candidate peut toutefois être légitime s'il s'agit, par exemple, de repourvoir un poste de médiateur culturel pour une association oeuvrant en faveur de l'intégration des personnes migrantes (*Tendenzbetrieb*)[71].

L'admissibilité des questions variera selon le niveau hiérarchique du poste[72]. Une personne pressentie pour occuper une position dirigeante peut être interrogée de façon plus étendue, notamment sur ses *hobbies*, susceptibles de révéler « son goût de l'effort ou son ouverture

66 Voir les instructions du Conseil fédéral du 22 janvier 2003 pour la réalisation de l'égalité des chances entre femmes et hommes dans l'administration fédérale, ch. 423, FF 2003 1332.

67 A titre d'illustration, voir un arrêt rendu par le Tribunal des prud'hommes de Lausanne le 1er juin 2005, *in* : JAR 2006 p. 531 (refus d'embauche d'une veilleuse de nuit en raison de sa couleur de peau).

68 Voir, parmi d'autres, DUNAND, N 44 *ad* art. 328b CO, qui renvoie notamment au TF, 2C_103/2008 du 30 juin 2008, c. 6.2.

69 DUNAND, N 46 *ad* art. 328b CO.

70 A titre d'illustration, voir une affaire résumée sur www.gleichstellungsgesetz.ch, ZH/71 (2002).

71 Pour d'autres exemples, voir notamment DUNAND, N 48 *ad* art. 328b CO.

72 MEIER, N 2088.

à de nouveaux défis »[73]. Il convient cependant de garder à l'esprit que les personnes assumant des responsabilités familiales parallèlement à une carrière professionnelle ont rarement le temps de s'adonner à des loisirs. Les questions relatives au « défi » que représente la conciliation entre travail et famille sont, en principe, interdites dans le cadre d'un entretien d'embauche. En effet, vu l'interdiction de discriminer prévue à l'article 3 LEg, les interrogations sur la vie familiale sont illicites au stade précontractuel. Il faut cependant réserver l'hypothèse, envisagée plus haut[74], où une personne candidate aborde spontanément le thème. En cours d'exécution du contrat de travail, en revanche, il est licite de traiter les données concernant la situation familiale, par exemple, pour déterminer un droit aux allocations familiales[75] ou fixer les heures de travail et de repos (art. 36 LTr).

Les questions relatives à une grossesse sont interdites par les articles 328b CO et 3 LEg, sous réserve des cas – exceptionnels – où celle-ci rendrait l'exécution du contrat de travail d'emblée impossible[76]. On pense, par exemple, au cas d'une entreprise qui aurait besoin d'engager une personne durant quelques mois, afin de remplacer une collaboratrice partie en congé maternité. En pareille situation, l'entreprise est en droit d'attendre de la candidate qu'elle annonce sa grossesse, sans attendre d'être interrogée à ce sujet[77]. La postulante devra alors convaincre l'employeuse de la faisabilité du remplacement.

De façon générale, lorsque l'état de santé est susceptible d'entraver la bonne exécution du contrat de travail, la personne candidate doit en informer les responsables du recrutement et répondre honnêtement aux questions qui sont posées à ce sujet[78]. En outre, une personne handicapée peut avoir intérêt à discuter, dès l'entretien d'embauche, des mesures qui permettraient d'adapter l'environnement professionnel à ses besoins (aménagement des locaux, des horaires ou du matériel informatique, par exemple)[79].

Les demandes concernant une maladie ou un handicap sans effet sur l'aptitude au travail sont, en principe, illicites[80]. Ainsi, des questions relatives à une infection par le VIH ne sont pas licites[81], sous réserve des cas où l'activité – dans un bloc opératoire, par exemple

---

73 AUBERT, p. 153 ; STREIFF/VON KAENEL/RUDOLPH, N 10 *ad* art. 328b CO considèrent, en revanche, illicites les questions afférentes aux hobbies.

74 Partie III, lettre A.

75 PORTMANN/RUDOLPH, N 9 *ad* art. 328b CO ; PÄRLI, N 24 *ad* art. 328b CO.

76 Pour plus d'explications, voir en particulier RUDOLPH, p. 80 s ; ÜBERSCHLAG, pp. 181-213.

77 LEMPEN, N 23-24 *ad* art. 3 LEg, avec les références.

78 ATF 132 II 161, c. 4.2. Voir, notamment, MEIER, N 2094 et 2101 ; PFPDT, Guide, p. 9 ; GEISER/MÜLLER, p. 89.

79 Voir l'art.12 OHand.

80 MEIER, N 2095 ; STREIFF/VON KAENEL/RUDOLPH, N 10 *ad* art. 328b CO.

81 TF, 2C_103/2008 du 30 juin 2008, c. 6.2.

– présente un risque de contagion élevé, susceptible d'être réduit par l'adoption de mesures d'hygiène particulières[82].

Lorsqu'une question illicite lui est posée, la personne candidate a le droit de refuser d'y répondre ou de mentir[83].

C. Recherche de données sur Internet

1. Généralités

En principe, les informations qui n'ont pas le droit d'être récoltées dans le cadre d'un entretien d'embauche n'ont pas non plus le droit de l'être via une recherche sur Internet.

L'article 328b CO, selon lequel seules les données portant « sur les aptitudes du travailleur à remplir son emploi » peuvent être traitées par les responsables du recrutement, limite fortement leur droit de se livrer à un *screening* des personnes candidates sur Internet[84].

2. Réseaux sociaux

Le traitement d'informations mises à disposition par la personne candidate sur des réseaux sociaux professionnels, comme LinkedIn, est généralement considéré comme admissible[85]. La plupart du temps, en effet, les personnes qui publient leur profil sur ces réseaux souhaitent précisément que celui-ci soit utilisé en vue d'un recrutement[86].

En revanche, l'utilisation de données personnelles figurant sur des réseaux sociaux privés, non professionnels, comme Facebook, pose problème sous l'angle de l'article 328b CO et des principes généraux de protection des données[87].

---

82 Voir en particulier RUDOLPH, pp. 66 s ; PÄRLI, N 26 *ad* art. 328b CO, qui cite un arrêt du Tribunal supérieur du canton de Zurich LA110040 du 8 avril 2013, selon lequel, avant le début du contrat, un footballeur professionnel infecté par le VIH n'est pas tenu d'en informer son club. Selon GEISER/MÜLLER, p. 88, il n'existe aucun métier où le risque de contagion subsisterait malgré le respect des prescriptions d'hygiène nécessaires.

83 Voir, notamment, DUNAND, N 50 *ad* art. 328b CO, avec les références.

84 Dans ce sens, voir, notamment, WILDHABER/HÄNSENBERGER pp. 325-327, qui précisent que l'art. 328b CO l'emporte l'art. 12 al. 3 LPD (selon lequel « il n'y a pas atteinte à la personnalité lorsque la personne concernée a rendu les données accessibles à tout un chacun et ne s'est pas opposée formellement au traitement »).

85 WILDHABER/HÄNSENBERGER, p. 327 avec les références.

86 AUBERT/DELLEY, p. 147.

87 Voir FLÜCKIGER, p. 75.

Selon le Comité des ministres du Conseil de l'Europe, « les employeurs devraient s'abstenir d'exiger ou de demander à un employé ou un candidat à l'emploi d'avoir accès à des informations que celui-ci partage avec d'autres en ligne, notamment sur des réseaux sociaux »[88]. L'exposé des motifs précise que lorsque l'accès au compte « d'un candidat à l'emploi sur un réseau social est restreint, l'employeur n'a pas le droit de demander à y avoir accès », par exemple en priant la personne candidate « de lui communiquer ses identifiants de connexion »[89]. Une telle pratique viole la sphère privée et entraîne un risque de discrimination notamment parce qu'elle permet d'obtenir des réponses à des questions prohibées lors d'un entretien d'embauche, comme celles relatives à l'orientation sexuelle[90] ou à l'identité de genre.

À cet égard, le Comité des ministres du Conseil de l'Europe recommande qu'une attention particulière soit « accordée à la protection efficace du droit à la vie privée des personnes transgenres dans le contexte du travail, en particulier en ce qui concerne les candidatures à un emploi, de manière à éviter la divulgation inutile de l'historique de leur genre ou de leur ancien nom à l'employeur et aux autres employés »[91].

3. Moteurs de recherche

La *googlelisation* des personnes candidates est illicite. En effet, lors d'une telle recherche, il est impossible, en pratique, de trier les informations de façon à ne tenir compte que des données dont le traitement est autorisé par l'article 328b CO[92]. Un tel procédé viole les principes de proportionnalité et de finalité (art. 4 LPD), « même si la personne concernée est préalablement informée »[93].

Dans l'hypothèse où la personne visée aurait donné son consentement, la question se pose de savoir si celui-ci a pu être donné librement. En effet, « quel candidat voulant garder ses chances d'obtenir le poste refusera la *googlelisation*»[94]? De plus, comme expliqué plus

88 Recommandation CM/Rec(2015)5 du Comité des Ministres aux Etats membres sur le traitement de données à caractère personnel dans le cadre de l'emploi du 1er avril 2015, chiffre 5.3.

89 Exposé des motifs de la Recommandation CM/Rec(2015)5, document CM(2015)32 addfinal, chiffre 46.

90 Dans ce sens, AUBERT/DELLEY, p. 148.

91 Recommandation CM/Rec(2010)5 du Comité des Ministres aux Etats membres sur des mesures visant à combattre la discrimination fondée sur l'orientation sexuelle ou l'identité de genre du 31 mars 2010, chiffre 30. Sur le droit de chaque personne à ce que des informations la concernant soient « oubliées » par les moteurs de recherche, voir un arrêt CJUE, *Google Spain SL, Google Inc. c. Agencia Española de Protección de Datos (AEPD), Mario Costeja González*, C-131/12 du 14 mai 2014.

92 FLUECKIGER, p. 81.

93 FLUECKIGER, p. 82.

94 FLUECKIGER, p. 88.

haut[95], une personne candidate ne pourra consentir valablement au traitement de données sans rapport avec ses aptitudes professionnelles que si la dérogation est dans son propre intérêt. « Or, les recherches sur Internet ne sont pas effectuées pour trouver des qualités dont le candidat aurait oublié de se vanter, mais uniquement pour essayer de s'assurer qu'il est le plus irréprochable possible, en s'immisçant dans sa vie privée »[96].

Enfin, le fait de se renseigner sur une personne candidate en entrant son nom dans un moteur de recherche pose problème également au regard du principe de l'exactitude des données (art. 5 LPD)[97]. En effet, les données qui se trouvent sur Internet ne sont pas nécessairement correctes et s'avèrent souvent incomplètes ou stéréotypées. Sur l'encyclopédie en ligne Wikipédia, par exemple, les articles au sujet de femmes célèbres sont plus rares et mettent davantage l'accent sur les aspects de leur vie privée que sur leur apport intellectuel[98]. De façon générale, les femmes apparaissent dans les médias beaucoup moins souvent que les hommes et sont rarement présentées comme des expertes sur le plan professionnel[99]. Dès lors, une décision d'embauche fondée sur la façon dont les personnes candidates sont présentées sur Internet peut s'avérer discriminatoire au sens de l'article 3 LEg.

IV. Conclusion

Malgré leur histoire différente, le droit relatif à la protection des données et le droit antidiscriminatoire poursuivent des buts similaires et considèrent comme « sensibles » en grande partie les mêmes données, notamment l'origine ethnique (sous la qualification « race »), le handicap (rattaché à la « santé »), l'orientation sexuelle (comprise dans la « sphère intime ») et le sexe (qui peut, dans certains cas[100], aussi faire partie de la « sphère intime »).

---

95 Partie II, lettre D, chiffre 2.

96 FLUECKIGER, p. 89.

97 FLUECKIGER, pp. 83 s ; PÄRLI, N 28 *ad* art. 328b CO.

98 Voir à ce sujet la Newsletter n° 20 du service de l'égalité de l'Université de Genève téléchargeable sur la page « Wikipédia : qui parle de quoi ? », disponible en ligne sur : www.unige.ch/rectorat/egalite/archives/evenements/wikipedia/, (consulté le 8.1.2017).

99 Voir la Recommandation CM/Rec(2013)1 du Comité des ministres aux Etats membres sur l'égalité entre les femmes et les hommes et les médias du 10 juillet 2013. Voir en particulier le chiffre 4 qui recommande d'inciter les médias « à promouvoir une image, un rôle et une visibilité des femmes et des hommes sans stéréotypes ».

100 Voir les explications données *supra* Partie II, lettre D, chiffre 1.

Le traitement de données personnelles sensibles à l'embauche peut être un préalable nécessaire à la mise en œuvre de mesures positives visant l'intégration professionnelle de certains groupes sociaux sous-représentés. Sous réserve de ce cas particulier, le droit antidiscriminatoire, à l'instar des normes de protection des données, n'admet que de façon restrictive le traitement de données sensibles lors d'un recrutement.

Dans le cadre d'une procédure de sélection, les deux régimes juridiques se complètent. Un renforcement du droit en matière de protection des données renforce la protection contre les discriminations et inversement.

À cet égard, il est intéressant d'observer que le rapport explicatif relatif à l'avant-projet de la loi révisée sur la protection des données indique qu'« aucune conséquence sur l'égalité entre hommes et femmes n'est à signaler »[101]. Quoi qu'il en soit, dans ce domaine, comme dans celui de la protection des données, le Parlement fédéral devra prochainement décider de la façon dont il entend améliorer l'accès des individus à la justice[102].

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-e.

AUBERT CAROLE/DELLEY RÉGINE, Utilisation des réseaux sociaux par les travailleurs et les employeurs, *in* : Jean-Philippe Dunand/Pascal Mahon (éds.), Internet au travail, Genève/Zurich/Bâle 2014, pp. 131-162.

AUBERT GABRIEL, La protection des données dans les rapports de travail, *in* : Gabriel Aubert et al., Journée 1995 de droit du travail et de la sécurité sociale, Zurich 1999, pp. 145-191.

AUBERT GABRIEL, Commentaire de l'art. 328b CO, *in* : Luc Thévenoz/Franz Werro (éds.), Commentaire romand, Code des obligations I, 2e édition, Bâle 2012.

AUBERT GABRIEL, Les rapports entre le droit privé et le droit public – Quelques étapes, préface, *in* : Jean-Philippe Dunand/Pascal Mahon/Stéphanie Perrenoud (éds.), Le droit de la relation de travail à la croisée des chemins : Convergences et divergences entre le droit privé du travail et le droit de la fonction publique, Genève/Zurich/Bâle 2016 (cité : AUBERT, préface).

DUNAND JEAN-PHILIPPE, Commentaire de l'art. 328b CO, *in* : Jean-Philippe Dunand/Pascal Mahon (éds.), Commentaire du contrat de travail, Berne 2013, pp. 317-355.

DUNAND JEAN-PHILIPPE, L'interdiction de la discrimination à l'embauche dans la Loi fédérale sur l'égalité (LEg), *in* : Jean-Philippe Dunand/Karine Lempen/Pascal Mahon (éds.), L'égalité entre femmes et hommes dans les relations de travail, Zurich 2016.

101 Rapport explicatif, p. 104.

102 Voir *supra* Partie II, lettre D, chiffre 3.

EMMENEGGER SUSAN, Feministische Kritik des Vertragsrechts : eine Untersuchung zum schweizerischen Schuldvertrags- und Eherecht, thèse, Fribourg 1999.

FLUECKIGER CHRISTIAN, La googlelisation des employés respecte-t-elle les principes de la protection des données ?, *in* : Jean-Philippe Dunand/Pascal Mahon (éds.), Internet au travail, Genève/Zurich/Bâle 2014.

GEISER THOMAS/MÜLLER ROLAND, Arbeitsrecht in der Schweiz, 3e édition, Berne 2015.

LE MÉTAYER DANIEL/LE CLAINCHE JULIEN, Données personnelles, vie privée et non-discrimination : des protections complémentaires, une convergence nécessaire, *in* : Revue Lamy Droit de l'immatériel, 90/2013, pp. 80-95.

LEMPEN KARINE, Commentaire de l'art. 3 LEg, *in* : Gabriel Aubert/Karine Lempen (éds.), Commentaire de la loi fédérale sur l'égalité, Genève 2011.

MEIER PHILIPPE, Protection des données, Fondements, principes généraux et droit privé, Berne 2010.

OFFICE FÉDÉRAL DU PERSONNEL, Guide. Qualité du processus de recrutement du personnel. Recrutement non discriminatoire, Berne 2015 (cité : OFPER).

SCHÖNENBERGER SILVIA/FIBBI ROSITA, Lutte contre les discriminations à l'embauche, Les mesures volontaires mises en œuvre par les employeurs en Suisse, Berne 2011.

STREIFF ULLIN/VON KAENEL ADRIAN/RUDOLPH ROGER, Arbeitsvertrag – Praxiskommentar zu Art. 319-362 OR,7e édition, Zurich/Bâle/Genève 2012.

PÄRLI KURT, Aids : Datenschutz und Diskriminierung, *in* : Digma 2003, pp. 127 ss.

PÄRLI KURT, Commentaire de l'art. 328b CO, *in* : Bruno Baeriswyl/Kurt Pärli (éds.), Datenschutzgesetz (DSG) - Handkommentar, Berne 2015.

PRÉPOSÉ FÉDÉRAL À LA PROTECTION DES DONNÉES ET À LA TRANSPARENCE, Guide pour le traitement des données personnelles dans le secteur du travail, Berne 2014 (cité : PFPDT, Guide).

PORTMANN WOLFGANG/RUDOLPH ROGER, Commentaire de l'art. 328b CO, *in* : Heinrich Honsell/Nedim Peter Vogt/Rolf Watter (éds.), Obligationenrecht I – Basler Kommentar, 6e édition, Bâle 2015.

RUDOLPH ROGER, Stellenbewerbung und Datenschutz, thèse, Berne 1997.

SCHEFER MARKUS/HESS-KLEIN CAROLINE, Droit de l'égalité des personnes handicapées, Berne 2013.

ÜBERSCHLAG JAKOB, Die Anstellungsdiskriminierung aufgrund des Geschlechts im privatrechtlichen Arbeitsverhältnis (Art. 3 Abs. 2 GIG) : unter besonderer Berücksichtigung des europäischen Rechts, thèse, Zurich 2009.

WALDMANN BERNHARD, Das Diskriminierungsverbot von Art. 8 Abs. 2 BV als besonderer Gleichheitssatz : unter besonderer Berücksichtigung der völkerrechtlichen Diskriminierungsverbote einerseits und der Rechtslage in den USA, in Deutschland, Frankreich sowie im europäischen Gemeinschaftsrecht anderseits, thèse, Berne 2003.

WERMELINGER AMÉDÉO, Datenschutz und Gleichstellungsgesetz : Wieso sich Frauen für ihre Privatheit interessieren müssten, *in* : AJP 11/2006, pp. 1446 ss.

WILDHABER ISABELLE/HÄNSENBERGER SILVIO, Internet am Arbeitsplatz : ausgewählte arbeitsrechtliche Fragestellungen, *in* : ZBJV 5/2016, pp. 307 ss.

MARIE MAJOR

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

Sommaire

		Page
I.	Introduction	288
II.	Portée du droit d'accès	289
	A. Fondements du droit d'accès	289
	B. Notion de fichier	290
	1. Dossier personnel : une définition souple	291
	a) Exemples de données traitées	291
	b) Délimitations quant au contenu	292
	c) Documents non contenus dans le dossier personnel de l'employé	293
	2. Fichier à l'ère du numérique	293
	C. Restrictions du droit d'accès	296
	1. Notes personnelles (art. 2 al. 2 let. a LPD)	296
	2. Abus de droit (art. 2 al. 2 CC)	297
	3. Restrictions au droit d'accès découlant de l'article 9 LPD	297
	a) Loi au sens formel (art. 9 al. 1 let. a LPD)	298
	b) Intérêts prépondérants d'un tiers (art. 9 al. 1 let. b LPD)	298
	c) Intérêts prépondérants de l'employeur (art. 9 al. 4 LPD)	300
III.	Modalités du droit d'accès	301
	A. Aspects temporels	301
	B. Requête en droit d'accès auprès de l'employeur	302
	1. Forme de la requête	302
	2. Contenu de la requête	302
	C. Réponse de l'employeur	303
	1. Requête acceptée	303
	a) Forme de la réponse	303
	b) Frais	305
	2. Requête rejetée	305
IV.	Conclusion	305
Bibliographie		306

I. Introduction

À l'ère du « Big Data », où certains érigent Edward Snowden en véritable héros des temps modernes et où des données bancaires sont vendues à des Etats en échange de sommes colossales, un seul constat s'impose : la donnée personnelle est devenue l'or noir du XXI^{ème} siècle. Parallèlement à cette valorisation, la volonté individuelle de maîtriser ses données personnelles et l'attente d'une protection étatique accrue dans ce domaine s'accentuent.

Les rapports de travail ne sont pas épargnés par cette problématique. En effet, si les nouvelles technologies permettent aux entreprises d'optimiser leur rendement en adoptant une organisation du travail plus structurée et une communication plus fluide, l'employé moderne voit ses données personnelles plus facilement stockées et conservées par son employeur. Sa personnalité en devient ainsi de plus en plus exposée.

Le dossier personnel constitue le lieu principal où l'employeur collecte et conserve les données de son employé.

En Suisse, toute personne a le droit de déterminer elle-même si et dans quels buts des informations à son sujet peuvent être traitées[1]. Ce droit fondamental à l'autodétermination en matière informationnelle découle des articles 8 § 1 de la Convention européenne des droits de l'homme (CEDH)[2] et 13 al. 2 de la Constitution fédérale (Cst.[3])[4].

Plusieurs droits spécifiques le composent, notamment, le droit de connaître l'existence de données personnelles, le droit de les consulter, de faire rectifier des données inexactes ou de faire radier ses propres données, le droit de s'opposer au traitement de ses données et le droit à la sécurité des données[5].

Le droit d'accès, institution-clé de la protection des données[6], constitue ainsi une prérogative du droit à l'autodétermination dans le traitement de données, car seule la personne ayant connaissance des données qui sont traitées sur son compte peut les faire rectifier, détruire ou en contester l'exactitude et ainsi protéger efficacement sa personnalité.

---

1 ATF 138 II 346, c. 8. 2, *in* : JdT 2013 I 71.

2 RS 0.101.

3 RS 101.

4 ATF 140 I 381, c. 4.1 ; 138 II 346, c. 8.2, *in* : JdT 2013 I 71 ; pour plus de détails, voir FLÜCKIGER, p. 849 ; MEIER, N 15 ss, p. 65.

5 FLÜCKIGER, p. 851.

6 Message du Conseil fédéral concernant la loi fédérale sur la protection des données (LPD) du 23 mars 1998 (Message LPD), FF 1988 II 421 (460).

A travers la présente contribution, nous examinerons le droit d'accès de l'employé à son dossier personnel en analysant sa portée (Partie II) puis en définissant les modalités de son exercice (Partie III).

II. Portée du droit d'accès

A. Fondements du droit d'accès

Sur le plan interne, la Loi fédérale sur la protection des données du 19 juin 1992 (LPD)[7] concrétise le droit à l'autodétermination en matière informationnelle. Elle permet de protéger la personnalité et les droits fondamentaux des personnes faisant l'objet d'un traitement de données notamment par des personnes privées physiques ou morales[8].

Conscient de la vulnérabilité particulière du travailleur notamment en raison du rapport de dépendance à l'employeur pendant une supposée longue durée[9], le législateur a introduit dans le Code des obligations l'article 328b CO[10] parallèlement à l'entrée en vigueur de la LPD. Cet article de nature relativement impérative[11] règlemente les questions liées à la protection des données dans le contrat de travail. Il détermine la nature des informations que l'employeur est en droit de traiter sur ses employés[12].

Bien qu'historiquement envisagé, le législateur a toutefois renoncé à créer un droit d'accès spécifique à l'employé[13] et s'est contenté de renvoyer aux dispositions de la LPD (art. 328b *i.f.* CO)[14].

Le droit d'accès de l'employé se fonde ainsi sur l'article 8 al. 1 et 2 LPD à teneur duquel :

> « *Toute personne peut demander au maître d'un fichier si des données la concernant sont traitées.*
>
> *Le maître du fichier doit lui communiquer :*

7 RS 235.1.
8 Art. 1 et 2 al. 1 let. a LPD.
9 Message LPD, FF 1988 II 421 (494).
10 RS 220.
11 Cf. art. 362 al. 1 CO.
12 Message LPD, FF 1988 II 421 (494).
13 Un alinéa 3 dédié au droit d'accès de l'employé était initialement prévu. Pour en savoir plus, voir MEIER, N 2024, p. 647.
14 Art. 328b *i.f.* CO.

a. ***toutes les données la concernant*** *qui sont* ***contenues dans le fichier***[15]*, y compris les informations disponibles sur l'origine des données ;*

b. le but et éventuellement la base juridique du traitement, les catégories de données personnelles traitées, de participants au fichier et de destinataires de données ».

Selon cette définition, l'employé ne peut demander l'accès qu'aux données le concernant à l'exclusion de données concernant d'autres personnes, comme par exemple ses collègues de travail[16]. Par ailleurs, les données doivent être contenues dans un fichier.

Le droit d'accès étant conçu de manière large, toute renonciation anticipée est nulle selon l'article 8 al. 6 LPD.

Toutefois, ce droit n'est pas absolu et l'employeur peut refuser ou restreindre la communication des renseignements demandés, voire en différer l'octroi, à certaines conditions.

Nous analyserons premièrement la notion de fichier (section B) telle que mentionnée à l'article 8 al. 2 let. a LPD en la mettant en rapport avec le dossier personnel de l'employé (sous-section 1) puis nous traiterons des motifs de restrictions du droit d'accès (section C).

B. Notion de fichier

À rigueur de texte de l'article 8 al. 2 LPD, l'employé ne peut avoir accès qu'aux fichiers détenus par l'employeur (« données contenues dans le fichier ») à l'exclusion de données volatiles non contenues dans un fichier.

La notion de fichier (*Datensammlung, collezione di dati*) est définie à l'article 3 let. g LPD comme un « ensemble de données personnelles dont la structure permet de rechercher les données par personne concernée ». Les fichiers ont pour fonction de rassembler les données au cours de leur collecte, puis d'en assurer une conservation ordonnée à moyen ou long terme[17].

La LPD étant « atechnologique », le fichier peut aussi bien être physique (papier) qu'informatique[18].

---

15 Nous mettons en exergue.

16 Dans une jurisprudence cantonale tessinoise parue au JAR 2015 p. 537, le Tribunal d'appel a refusé l'accès d'une cheffe d'équipe aux comptes rendus et plannings des collaborateurs sous sa supervision, considérant qu'il s'agissait de données de tiers appartenant à l'employeur en fondant son argumentation sur l'article 328b CO et non sur la LPD.

17 MEIER, N 559, p. 240 et les références citées.

18 DUNAND, N 68 *ad* art. 328b CO, p. 338 ; MEIER, p. 680.

En matière de droit du travail, le fichier principal est celui que l'usage qualifie de « dossier personnel » de l'employé.

Si la notion de « dossier personnel » est comprise de tous, que contient-il réellement ou devrait-il contenir ? À quelles données l'employé peut-il avoir accès ? Nous tenterons de répondre à ces questions dans la sous-section suivante.

1. Dossier personnel : une définition souple

En droit privé suisse[19], il n'existe pas d'obligation légale de constituer un dossier personnel de l'employé et l'employeur demeure libre d'y inclure les données qu'il juge nécessaires. Or, avec MEYER, nous considérons qu'il s'agit d'une obligation indirecte (*indirekte Pflicht*) de l'employeur[20]. En effet, un tel procédé permet à ce dernier de remplir ses obligations légales découlant du contrat de travail comme le paiement du salaire ou des charges sociales.

La jurisprudence ne définit pas la notion de dossier personnel. La doctrine, quant à elle, s'accorde à dire que le dossier personnel comporte les données **concernant le travailleur dans ses rapports de travail** avec l'employeur de la naissance, au déroulement et à la fin des rapports de travail[21].

a) Exemples de données traitées

Dès les prémisses des rapports de travail, le candidat remet des données le concernant à son futur employeur, telles ses coordonnées, adresse, dossier de candidature, curriculum vitae (comprenant notamment son parcours scolaire et professionnel, ses connaissances linguistiques, ses hobbies), ses références et certificats de travail, et parfois même un extrait de son casier judiciaire, une attestation de non poursuite ou un test graphologique (consenti) censé révéler les traits de sa personnalité.

En cas d'engagement du candidat, ces informations sont généralement conservées par l'employeur et un « dossier personnel » est créé. D'autres données sont alors requises,

---

19 A l'inverse de certains droits cantonaux réglementant les rapports de la fonction publique et mentionnant expressément le dossier personnel et les actes à y inclure. Voir par exemple : l'Ordonnance sur le personnel (OPers) du canton de Berne (RS/BE 153.011.1), le Verordnung zum Personalgesetz (Personalverordnung) du canton de Bâle-Campagne du 19.12.2000 (RS/BL 150.11) ou les articles 34ss du *Personalgesetz* (PG) du canton de Zurich du 27.09.1998 (RS/ZH 177.10).

20 MEYER, p. 351.

21 MEIER, N 2116, p. 680 ; WYLER/HEINZER, p. 340 ; DUNAND, 68 *ad* art. 328b CO, p. 338 ; CARRUZZO, p. 329 ; STREIFF/VON KAENEL/RUDOLPH, N 13, p. 611 ; RUDOLPH, p. 1673.

comme les coordonnées bancaires de l'employé, son numéro AVS, le nom d'une personne de contact en cas d'urgence, une éventuelle demande d'allocations familiales, etc.

Puis, au cours des rapports de travail, l'employeur diligent établit des décomptes d'heures de travail et d'absence ou de vacances de son employé. Il peut aussi être amené à détenir des certificats médicaux justifiant les absences de son collaborateur ou des copies des déclarations d'accident.

Plus délicat mais souvent déterminant en cas de litige, les parties au contrat de travail ont tout intérêt à documenter et à garder une trace de l'évolution de leurs rapports de travail s'agissant de leur satisfaction quant aux prestations réciproques. Aussi, les évaluations des performances, les correspondances échangées au sujet d'événements particuliers[22], les avertissements, les éventuelles plaintes devraient être conservés soigneusement. La bonne tenue d'un dossier personnel contribue ainsi à la transparence et à l'optimisation du droit d'accès dans l'intérêt des deux parties. À notre sens, devrait figurer au dossier personnel tout élément ayant servi à prendre une décision impactant les rapports de travail.

La lettre de démission ou de licenciement, le certificat de travail ou les échanges postérieurs de correspondance viendront clôturer le dossier personnel.

b) Délimitations quant au contenu

Il convient toutefois de préciser que seules les données que l'employeur est habilité à traiter au sens de l'article 328b CO figureront au dossier personnel, soit les données *concernant le travailleur 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.*

Les données remplissant les critères précités sont présumées ne pas porter atteinte à la personnalité du travailleur[23].

La notion de « données personnelles » ou « données » est définie à l'article 3 let. a LPD comme « toutes les informations qui se rapportent à une personne identifiée ou identifiable ». Ces données peuvent être objectives (p. ex. une expérience professionnelle) ou subjectives (soit un jugement de valeur, p. ex. l'appréciation portée sur le travail d'un employé)[24].

En vertu du principe d'exactitude (*Datenrichtigkeit*) prévu à l'article 5 al. 1 LPD, les données figurant au dossier personnel doivent être correctes, soit refléter de manière correcte, actuelle et objective les faits ou autres circonstances se rapportant à la personne

22 PFPDT, p. 12.
23 ATF 130 II 425, c. 3.3.
24 MEIER, N 747, p. 289.

concernée[25]. À ce propos, le Préposé fédéral recommande à l'employeur de trier régulièrement – tous les deux ans en général – les dossiers du personnel en y retirant les documents inutiles ou inexacts[26].

Aussi, rappelons que seuls les faits peuvent être exacts ou inexacts, et non les jugements de valeur[27]. Cependant, les jugements de valeurs mixtes (*gemischtes Werturteil*), doivent être considérés comme des faits et, partant, être exacts[28]. Un jugement de valeur est dit mixte lorsqu'il est si étroitement lié à des faits qu'il forme un tout avec eux. Tel sera le cas lorsque l'expression d'une opinion comporte une allégation de fait ou constitue le prolongement d'une analyse portant sur les faits[29].

L'existence-même d'une critique ou d'un jugement de valeur constitue quant à elle un fait[30].

c) Documents non contenus dans le dossier personnel de l'employé

Il ressort des développements précédents que la constitution et le contenu du dossier personnel dépendent de la diligence et du bon vouloir de l'employeur. Eu égard à cette prérogative, l'employé peut-il avoir accès à d'autres données que celles figurant dans son dossier personnel ?

Pour répondre à cette question, il est nécessaire de comprendre la notion de dossier personnel au sens matériel et non formel[31]. La qualification par l'employeur de « dossier personnel » n'est ainsi pas décisive et l'employé peut avoir accès à d'autres fichiers détenus par l'employeur contenant ses données. Tel sera le cas des dossiers dits « gris », soit les dossiers non officiels tenus au sujet de l'employé[32].

2. Fichier à l'ère du numérique

S'il est plus aisé d'appréhender la notion de fichier (au sens de structure permettant de rechercher les données par personne concernée) s'agissant du dossier physique (papier)

---

25 MEIER, N 745, p. 289 et les références citées.

26 PFPDT, p. 12.

27 *Ibidem*.

28 Cf. action en rectification art. 15 al. 1 LPD, voir la contribution de Me AURÉLIEN WITZIG dans le présent ouvrage, pp. 31 s.

29 TF 5C.135/2003 du 15 septembre 2003, c. 3.2.1 ; MEIER, N 747, p. 289 ; STEINAUER/FOUNTOULAKIS, N 630, p. 251 ; STREIFF/VON KAENEL/RUDOLPH, N 16, p. 618.

30 MEIER, N 748, p. 289.

31 MEIER, N 211, p. 680 ; STREIFF/VON KAENEL/RUDOLPH, N 13, p. 611 ; RUDOLPH, P. 1673.

32 ATF 125 II 417, c. 4b, *in* : JdT 2001 I p. 322 ; MEIER, N 2117, p. 680 ; RUDOLPH, p. 1673 ; STREIFF/VON KAENEL/RUDOLPH N 15, p. 614.

d'un employé, l'application de cette notion au domaine informatique nous semble plus délicate. Cette problématique mérite d'être approfondie puisqu'à ce jour, 98% des informations sont enregistrées sous forme numérique[33] et donc dématérialisée.

Aussi, grâce aux fonctions de « recherche », l'ordinateur ou la boîte email de l'employé, le serveur informatique ou le *cloud* de l'entreprise représentent-ils des fichiers au sens de la LPD ? Autrement dit l'employé pourrait-il demander l'accès à l'ensemble de ses données y figurant ?

La doctrine semble répondre par la négative en se basant sur le critère de l'action, voire de la volonté du maître de fichier.

Selon MEIER, seules les données présentant entre elles un lien thématique logique peuvent être qualifiées de « fichier » à l'exclusion des données rassemblées par le hasard technique ou matériel[34]. En matière de droit du travail, cet auteur préconise de permettre l'accès aux données portant « sur les rapports de la personne concernée avec l'employeur »[35]. Cette solution présente l'avantage de soustraire du droit d'accès l'ensemble du travail accompli informatiquement par l'employé tels les emails ou les documents rédigés sur ordinateur.

Pour PAGE, si une clé de recherche existe ou peut être mise en place facilement, il incombe au maître de fichier de s'organiser pour permettre le droit d'accès. Ce devoir d'organisation ne l'obligerait cependant pas à relier ou rattacher des données qu'il ne prévoirait pas d'utiliser de manière « personnelle »[36].

Selon le Tribunal administratif fédéral[37], ce qui est décisif, du point de vue de la protection des données, c'est que l'on puisse rechercher les données par personne concernée. S'agissant des traitements automatisés (soit informatiques), il n'est pas nécessaire que les clés d'accès soient constituées par des noms de personnes, tant les possibilités d'interrogation de ces banques de données sont nombreuses. En revanche, la jurisprudence semble exclure de la notion de fichier les ensembles de données qui, bien que permettant d'accéder à des données personnelles, nécessitent la mise en œuvre de moyens disproportionnés[38].

Au vu du perfectionnement constant des logiciels de recherche, ces considérations laissent songeurs. En effet, les techniques d'indexation deviennent de plus en plus pointues et,

---

33 CUKIER et MAYER-SCHÖNBERGER, p. 9.

34 MEIER, N 574, p. 244.

35 MEIER, N 2119, p. 681. En ce sens également, STREIFF/VON KAENEL/RUDOLPH, N 13, p. 611 et pp. 615 s.

36 PAGE, p. 124 ; PAGE, ZBI, p. 386 ; dans un sens similaire, MONNIER, pp. 169-170.

37 TAF A-4190/2009 du 29 novembre 2010, c. 3.2.

38 *Ibidem*.

grâce aux nouvelles technologies, l'employeur peut facilement rechercher des informations concernant son employé à travers des espaces de stockages de plus en plus grands et collecter, voire utiliser, des données personnelles à l'insu de celui-ci. Par exemple, en quelques clics de souris, il peut aisément évaluer le rendement quotidien d'un employé de bureau s'agissant du travail accompli informatiquement[39]. En réalité, le résultat d'une telle recherche ne figurera que rarement au dossier personnel « officiel » de l'employé.

S'il est illusoire et contre-productif d'envisager un accès à l'ensemble des données personnelles du travailleur, cette problématique souligne la nécessité pour les parties de documenter l'évolution de leur relation de travail avec précaution, en regroupant de manière transparente tous les éléments qui leur ont permis de prendre une décision impactant leurs rapports. Un tel procédé contribue à la réalisation du lien de confiance qui caractérise le contrat de travail.

Relevons enfin que l'avant-projet de loi fédérale sur la révision totale de la loi sur la protection des données et sur la modification d'autres lois fédérales prévoit de supprimer la notion de fichier (art. 3 AP-LPD)[40]. Ainsi, à teneur de cet avant-projet, la personne concernée pourra accéder « aux données personnelles traitées » sans égard à ce que celles-ci soient contenues dans un fichier[41]. Ce changement est intervenu pour tenir compte de l'évolution des nouvelles technologies qui permettent d'exploiter des données disséminées comme un fichier[42].

En contrepartie notamment de l'abandon de la notion de fichier, la notion de « profilage » devrait être introduite dans la nouvelle loi[43]. Le profilage se définit comme « toute exploitation de données personnelles ou non, consistant à analyser ou prédire les caractéristiques personnelles essentielles d'une personne, notamment son rendement au travail, sa santé, sa sphère intime, ou ses déplacements ». En cas de profilage, la personne concernée devra donner son consentement exprès[44]. A défaut d'un tel consentement, l'opération de profilage sera constitutive d'une atteinte à la personnalité[45].

À nos yeux, cette nouvelle solution adaptée à l'évolution des technologies permet de répondre aux problématiques mentionnées ci-avant et renforce la protection de la personnalité de l'employé.

---

39 A ce sujet voir ATMANI.

40 Rapport explicatif, p. 44 ; voir aussi la contribution de Mme CAMILLE DUBOIS dans le présent ouvrage, pp. 59 s.

41 Art. 20 al. 2 let. b AP-LPD.

42 Rapport explicatif, p. 44.

43 Art. 3 let. f AP-LPD.

44 Art. 4 al. 6 AP-LPD.

45 Art. 23 AP-LPD.

C. Restrictions du droit d'accès

Comme expliqué *supra*, le droit d'accès n'est pas un droit absolu et comporte certaines limitations. L'employeur peut refuser de communiquer tout ou partie des informations demandées ou en différer la communication.

Certaines restrictions générales découlent du champ d'application de la LPD, tel le traitement de données pour un usage personnel (sous-section 1)[46] ou de l'interdiction de l'abus de droit (sous-section 2).

Les autres restrictions résultent des dispositions topiques de l'article 9 LPD (sous-section 3).

1. Notes personnelles (art. 2 al. 2 let. a LPD)

La loi prévoit que les données personnelles traitées par une personne physique pour un usage exclusivement personnel et non communiquées à des tiers sont exclues du champ d'application de la LPD (art. 2 al. 2 let. a LPD). Ainsi, l'employé ne peut exiger l'accès aux notes de son supérieur hiérarchique à son sujet du moment que celles-ci demeurent personnelles.

La communication des données à des auxiliaires immédiats de l'auteur du traitement (p. ex. le secrétariat de l'employeur) n'est toutefois pas considérée comme une communication à des tiers[47].

Précisons ici que les documents pouvant être qualifiés d' « internes » à une personne morale ou de « confidentiels » (p. ex. un échange d'emails au sujet d'un collaborateur entre un supérieur hiérarchique et le responsable des ressources humaines), ne sont pas concernés par cette disposition mais peuvent faire l'objet d'un refus d'accès selon l'article 9 LPD[48].

Aussi, la notion d'usage personnel doit être interprétée restrictivement[49].

---

46 S'agissant de l'exclusion de l'application de la LPD aux procédures pendantes civiles pénales, d'entraide judiciaire internationale ainsi que de droit public ou administratif (art. 2 al. 2 let. c LPD), voir *infra* III A.

47 MEIER, N 384, p. 188.

48 MEIER, N 383, p. 187 ; RUDOLPH, p. 1679.

49 RUDOLPH, p. 1679.

2. Abus de droit (art. 2 al. 2 CC)

Le droit d'accès doit être exercé dans les limites de l'abus de droit de l'article 2 al. 2 du Code civil (CC)[50].

Il existe un abus de droit lorsque l'exercice du droit par le titulaire ne répond à aucun intérêt digne de protection, qu'il est purement chicanier ou, lorsque, dans les circonstances dans lesquelles il est exercé, le droit est mis au service d'intérêts qui ne correspondent pas à ceux que la règle est destinée à protéger. Ainsi, pourrait être qualifiée d'abusive, la requête ne visant qu'à nuire au débiteur de ce droit[51] ou ayant comme but exclusif d'espionner une (future) partie adverse et de se procurer des preuves normalement inaccessibles. Le droit d'accès n'est en effet pas destiné à faciliter les preuves ou à interférer dans le droit de procédure civile. Le caractère abusif d'une telle requête doit être apprécié selon le cas d'espèce[52].

En revanche, la requête d'une personne visant à obtenir les données le concernant en vue d'une éventuelle action en dommages-intérêts contre le maître du fichier n'est pas abusive[53]. Le Tribunal fédéral a admis le droit d'accès de deux clients ayant subi un dommage financier causé par les agissements d'un établissement bancaire, la requête visant à obtenir leurs « profils clients » ainsi que leurs objectifs d'investissement. Les deux clients avaient indiqué lors d'un échange de courriers que la demande d'accès était introduite en vue d'une demande en dommages et intérêts concernant des transactions[54].

Nous relevons que l'abus de droit, comme à l'habitude, n'est pas aisément admis par le Tribunal fédéral et qu'une personne peut demander l'accès à des documents constituant de futures preuves afin d'évaluer l'éventualité d'une action judiciaire[55].

3. Restrictions au droit d'accès découlant de l'article 9 LPD

À teneur de la loi, l'employeur peut refuser l'accès au dossier personnel lorsque :

1) une loi au sens formel le prévoit ;
2) les intérêts prépondérants d'un tiers l'exigent ;
3) ses intérêts prépondérants l'exigent et à condition qu'il ne communique pas les données à un tiers.

---

50 RS 210.
51 TF 4A_36/2010 du 20 avril 2010, c. 3.1.
52 ATF 138 III 425, c. 5.5, *in* : SJ 2013 I 81.
53 ATF 141 III 119, c. 7.1.1, *in* : SJ 2015 I 353 et ATF 138 III 425, c. 5.6, *in* : SJ 2013 I 81.
54 ATF 138 III 425, c. 5.6, *in* : SJ 2013 I 81.
55 En ce sens, AUBERT, p. 42 ; RUBIN, N 20, p. 104.

Ces motifs sont alternatifs et forment une liste exhaustive[56].

Le refus peut être partiel ou total et l'employeur peut également décider de différer la communication. Le choix entre ces trois possibilités s'effectue en tenant compte du principe de proportionnalité contenu à l'article 4 LPD.

a) Loi au sens formel (art. 9 al. 1 let. a LPD)

À teneur de l'article 9 al. 1 let. a LPD, l'employeur peut refuser l'accès au dossier personnel lorsqu'une loi au sens formel le prévoit.

La loi doit être comprise au sens de l'article 3 let. j LPD comme une loi fédérale ou une résolution d'organisation internationale contraignante pour la Suisse ou un traité de droit international approuvés par l'Assemblée fédérale et comportant des règles de droit.

À ce titre, le secret professionnel (art. 321 du Code pénal (CP)[57]) ou le secret bancaire (art. 47 de la Loi fédérale sur les banques et les caisses d'épargne (LB)[58]) constituent des bases légales formelles permettant de refuser l'accès[59].

La jurisprudence a toutefois retenu que ces secrets n'ont qu'une portée limitée ; d'une part, car l'employé demeure soumis aux secrets professionnel ou bancaire après la fin de ses rapports de travail[60] et, d'autre part, car le caviardage constitue souvent un moyen approprié pour préserver tout éventuel secret[61].

Partant, on ne saurait ainsi exclure totalement le droit d'accès en se basant sur l'invocation d'un secret.

b) Intérêts prépondérants d'un tiers (art. 9 al. 1 let. b LPD)

Le droit d'accès peut être refusé, restreint ou différé lorsque les intérêts prépondérants d'un tiers l'exigent (art. 9 al. 1 let. b LPD).

En droit du travail, cette disposition concerne principalement les cas de dénonciation d'un employé suite à des agissements répréhensibles (infraction pénale, actes de mobbing, ou simplement mauvaise conduite justifiant une sanction). Dans certaines situations,

---

56 Message LPD, FF 1988 II 421 (462) ; MEIER, N 1121, p. 402 ; HUSI-STÄMPFLI, N 15, p. 120.

57 RS 311.0.

58 RS 952.0.

59 MEIER, N 1139, p. 405 et les auteurs cités ; RUDOLPH, p. 1681.

60 Jugement de l'Arbeitsgericht de Zurich AH130073 du 23 juillet 2013, publié *in* : Entscheide des Arbeitsgerichtes Zürich 2013 ; arrêt de la Cour de justice genevoise ACJC/881/2014 c. 5.2 ; ATF 141 III 119, c. 7.4.

61 Arrêt de la Cour de justice genevoise ACJC/881/2014, c. 5.2.

l'employé incriminé aura pourtant un intérêt à connaître l'identité du dénonciateur et une pesée des intérêts en présence devra être effectuée.

À notre sens, les intérêts du dénonciateur justifieront en tout cas une limitation temporaire de l'accès, le temps de traiter la dénonciation, au moins aussi longtemps que nécessaire pour établir si les soupçons sont fondés[62].

Pour les autres cas, nous rejoignons MEIER qui établit une liste des conditions cumulatives auxquelles l'intérêt du dénonciateur à ne pas être identifié devrait être jugé comme prépondérant, soit lorsque[63] :

- le maître du fichier a légitimement garanti la confidentialité au dénonciateur et ce dernier pouvait de bonne foi s'y fier eu égard à la nature délicate de l'information ;
- l'information donnée ne pouvait être obtenue que par un cercle limité de personnes dont l'informateur faisait partie ;
- la levée de l'anonymat entraîne un risque pour l'intégrité physique ou psychique de l'informateur ou de ses proches ou met en danger de manière notable des biens immatériels ou économiques importants de l'intéressé (cas de l'employé dénonçant ses supérieurs hiérarchiques, risquant ainsi de se voir licencier).

À ce sujet, l'Arbeitsgericht de Zurich a refusé une requête d'accès portant sur la révélation du nom du collaborateur ayant dénoncé son supérieur hiérarchique car le témoignage avait été recueilli sous la garantie de l'anonymat. La banque avait cependant autorisé le supérieur à prendre connaissance du procès-verbal d'interrogatoire anonymisé de ladite personne[64].

Dans un autre cas, le même tribunal a accordé un droit d'accès à un employé bancaire licencié avec effet immédiat suite à une enquête interne diligentée en raison de plaintes émanant de clients. L'employé a pu prendre connaissance de tous les actes, documents, procès-verbaux, notes et rapports de l'enquête sous la forme anonymisée[65].

Ainsi, de manière générale, l'anonymisation des documents semble suffire à protéger les intérêts des tiers et l'employeur ne devrait pas refuser le droit d'accès sous peine d'une violation du principe de proportionnalité[66].

Enfin, lorsque le dénonciateur est également un employé, l'employeur bénéficie d'un double motif justificatif en vertu de son devoir de protection découlant de l'article 328 CO.

---

62 Du même avis, CARRANZA et MICOTTI, p. 85.

63 MEIER, N 1147, p. 407.

64 Jugement de l'Arbeitsgericht de Zurich AN110024 du 20 mars 2012, publié *in* : Entscheide des Arbeitsgerichtes Zürich 2012.

65 Jugement de l'Arbeitsgericht de Zurich AH130073 cité sous note 59.

66 ATF 141 III 119, c. 6.2.

Il peut invoquer tant l'article 9 al. 1 let. b LPD que l'article 9 al. 4 LPD car, en cas de violation de ce devoir, il sera tenu pour responsable.

c) Intérêts prépondérants de l'employeur (art. 9 al. 4 LPD)

L'employeur peut refuser ou restreindre la communication des renseignements demandés ou en différer l'octroi, dans la mesure où ses intérêts prépondérants l'exigent et à condition qu'il ne communique pas les données personnelles à un tiers (art. 9 al. 4 LPD).

L'intérêt de l'employeur ne doit pas simplement paraître digne de protection, mais il doit l'emporter sur l'intérêt de l'employé[67].

Parmi les exemples d'intérêts prépondérants, figurent les craintes d'un espionnage industriel, la mise en danger et les atteintes aux droits de la personnalité du débiteur du droit d'accès ainsi que les intérêts financiers prépondérants[68].

L'employeur peut également opposer un intérêt prépondérant pour tous les documents révélant ses intentions stratégiques, par exemple des documents relatifs à la planification des besoins en personnel, aux plans de carrière[69] ou des échanges concernant sa stratégie de défense en cas de conflit avec un employé[70].

Dans un arrêt concernant le droit de la fonction publique, le Tribunal fédéral a considéré (sous l'angle du droit d'être entendu de l'article 29 Cst.) que les emails échangés entre supérieurs hiérarchiques concernant un employé préalablement à son licenciement constituaient des actes internes de formation de volonté (*Willensbildung*) et n'étaient pas à inclure au dossier personnel[71]. Cette notion devrait être reprise pour les actes internes participant au processus décisionnel d'une personne morale.

Plus délicate est la question du droit d'accès à l'ensemble du dossier personnel en cas de relation conflictuelle avec l'employé, notamment suite à un licenciement. Dans un tel cas, l'employé peut avoir un intérêt évident à recevoir une copie intégrale de son dossier personnel afin de formuler certaines prétentions à l'encontre de son ancien employeur. À ce sujet, le Tribunal fédéral proscrit les requêtes en « *fishing expedition* », soit les recherches indéterminées de moyens de preuves[72]. Toutefois, comme indiqué *supra*[73], il ne considère pas comme abusive la requête visant à demander une copie du profil client dans

67 MEIER, N 1142, p. 406.
68 ATF 138 III 425, c. 6.1, *in* : SJ 2013 I 81.
69 PFPDT, p. 13.
70 CARRUZZO, p. 331 ; MEIER, N 1157, p. 410 ; DUNAND, N 79, p. 340 ; RUDOLPH, p. 1680.
71 TF 8C_467/2013 du 21 novembre 2013, c. 3.2.
72 ATF 141 III 119, c. 7.1.1.
73 *Supra* II C 2.

l'optique de faire valoir des futures prétentions[74]. Au vu de cette jurisprudence, l'employé formulant des prétentions à l'encontre de son employeur devrait ainsi pouvoir avoir accès à son dossier personnel[75].

Enfin, à teneur de la loi, l'employeur ne peut toutefois invoquer un intérêt prépondérant lorsqu'il communique ou a communiqué les données à un tiers. Une partie de la doctrine distingue les cas de communication volontaire de ceux où la communication est effectuée en vertu d'une obligation. Dans ce dernier cas, l'employeur pourrait toujours invoquer son intérêt prépondérant pour refuser l'accès[76]. La Cour de justice genevoise a rejeté cette interprétation élargie de l'article 9 al. 4 LPD, compte tenu de l'importance du droit d'accès et a indiqué qu'en cas de communication forcée, l'employeur ne peut faire valoir un intérêt prépondérant[77].

Ces constatations établies, nous analyserons les aspects fonctionnels du droit d'accès soit les aspects temporels et les modalités pratiques.

III. Modalités du droit d'accès

A. Aspects temporels

Le droit d'accès peut être invoqué en tout temps : avant les rapports de travail (cas du postulant)[78], pendant les rapports de travail et même après ceux-ci[79].

Aussi longtemps qu'il n'y a pas de procédure civile pendante, il est possible de demander des renseignements sur la base de la LPD sous réserve de l'abus de droit[80]. En effet, à teneur de l'article 2 al. 2 let. c LPD, la loi exclut de son champ d'application notamment les procédures pendantes civiles, pénales, publiques et administratives. À l'ouverture d'une telle procédure, les règles de procédure sont applicables et notamment le droit d'être entendu, le droit d'accéder au dossier et le droit de participer à l'administration des

74 ATF 138 III 425, c. 5.6, *in* : SJ 2013 I 81.

75 A ce sujet voir WYLER/HEINZER et leurs développements, p. 341.

76 MONNIER, p. 210.

77 Arrêt de la Cour de justice genevoise, ACJC/881/2014 précité.

78 La doctrine convient que le postulant dont la candidature n'a pas été retenue peut requérir un droit de consulter son dossier. A ce sujet voir AUBERT, p. 177 ; DUNAND, N 81 *ad* art. 328b CO, p. 341 ; MEYER, p. 354 ; RUDOLPH, p. 1673.

79 ATF 120 II 118, c. 3c, *in* : JdT 1995 I 141– arrêt rendu avant l'entrée en vigueur de la LPD.

80 ATF 138 III 425, c. 4.3, *in* : SJ 2013 I 81.

preuves[81]. Le but de cette disposition est d'éviter un concours objectif de normes entre le droit de procédure et la LPD.

En tant que droit de la personnalité, le droit d'accès est imprescriptible[82]. Or, en pratique, on ne saurait raisonnablement exiger de l'employeur qu'il conserve les données au-delà des délais de prescription de 5 ou 10 ans figurant aux articles 127 et 128 ch. 3 *i.f.* CO[83].

En cas de décès, les proches du défunt peuvent demander l'accès au dossier en vertu de l'article 1 al. 7 OLPD.

B. Requête en droit d'accès auprès de l'employeur

Le droit d'accès au dossier personnel n'intervient que sur requête de l'employé.

1. Forme de la requête

La loi ne réglemente pas strictement la forme de la requête. Celle-ci sera en règle générale écrite (art. 1 al. 1 OLPD) mais l'employeur demeure libre de définir les modalités de cet exercice. Il peut, par exemple, prévoir par contrat ou règlement interne que la demande d'accès lui soit adressée par voie électronique[84].

Dans les cas simples et non contentieux, une requête orale devrait suffire.

En pratique, pour des raisons de preuve et de respect des délais, l'employeur diligent préférera les requêtes écrites ou électroniques.

2. Contenu de la requête

L'employé peut formuler une requête globale ou ciblée en mentionnant le document qu'il souhaite consulter. Dans ce dernier cas, afin de faciliter les recherches de son employeur et, dans la mesure où l'employé en a connaissance, il devrait indiquer le nom du document ou le genre de données qu'il entend consulter. Avec DUNAND, nous convenons qu'à défaut de précision et dans la mesure où l'employé ignore en général si son employeur exploite

---

81 Message LPD, FF 1988 II 421 (450).

82 PAGE, p. 121 ; MEYER et les références citées, p. 354 ; MEIER, N 975, p. 364 ; RUDOLPH, p. 1676.

83 A ce sujet, voir les directives du Préposé fédéral sur la conservation des dossiers personnels : http://www.edoeb.admin.ch/dokumentation/00153/00393/00394/index.html?lang=fr (consulté le 07.01.16).

84 Dans un tel cas, l'employeur devra prévoir les mesures adéquates pour assurer l'identification de la personne concernée (but d'authentification de la personne requérante) et pour assurer la protection des données de tout accès de tiers non autorisés lors de la communication de renseignements (art. 1 al. 2 OLPD).

un ou plusieurs fichiers le concernant, il est présumé que sa requête constitue une demande globale valant pour tous les fichiers[85]. Cette solution présente l'avantage de garantir la bonne exécution du droit d'accès.

En principe, l'employé n'a pas à motiver sa requête ni à démontrer l'existence d'un intérêt digne de protection ou d'une atteinte effective ou potentielle à sa personnalité[86]. Cependant, il peut être parfois judicieux de motiver à ce stade le but de la requête afin d'anticiper un éventuel futur refus de l'employeur ou de justifier une requête pouvant *prima facie* paraître abusive. La motivation dépendra donc de la stratégie adoptée par le requérant[87].

L'employé doit toutefois démontrer un intérêt pour obtenir gratuitement accès à son dossier s'il a déjà exercé son droit dans les douze mois précédents la requête (art. 2 al. 1 let. b OLPD). Dans pareil cas, une motivation est alors essentielle.

C. Réponse de l'employeur

Dans les cas d'acceptation comme de refus, l'employeur a l'obligation de répondre à la requête en droit d'accès de l'employé.

L'employeur est tenu de fournir les renseignements ou de transmettre sa décision de refus dans un délai maximal de 30 jours dès réception de la requête. Si les renseignements ne peuvent être donnés dans les 30 jours, l'employeur en avertit l'employé en lui indiquant le délai dans lequel interviendra sa réponse (art.1 al. 4 OLPD).

1. Requête acceptée

a) Forme de la réponse

Si l'employeur accepte la requête, il dispose de quatre modes de communication : la forme écrite, la forme électronique, la consultation sur place ou la communication orale.

L'employé n'a pas de droit de consulter l'original de son dossier, sous réserve des cas d'abus de droit[88] et sauf si les parties en sont convenues ainsi (art. 1 al. 3 OLPD).

---

85 DUNAND, N 75 *ad* art. 328b CO, p. 339.

86 ATF 141 III 119, c. 7.1.1 ; jugement de l'Arbeitsgericht de Zurich du 26 juin 2006 c. 1.4, *in* : JAR 2007, p. 524 cité *in* : DUNAND, 75 *ad* art. 328b CO, p. 339.

87 Le PFPDT propose des modèles de courrier à l'adresse suivante : http://www.edoeb.admin.ch/oeffentlichkeitsprinzip/00901/00907/00908/index.html?lang=fr (consulté le 07.01.16).

88 On peut ainsi songer à des cas où l'authenticité des documents serait remise en question par l'employé.

La règle est en principe une communication par écrit, sous forme d'imprimé ou de photocopie (art. 8 al. 5 LPD).

Dans une jurisprudence récente[89] le Tribunal fédéral a rappelé cette règle et a jugé qu'il ne pouvait y être dérogé par l'acceptation d'un règlement interne interdisant aux employés d'une banque d'emporter des documents confidentiels chez eux[90]. En vertu de l'article 8 al. 6 LPD[91], les employés ne pouvaient renoncer à l'avance à la remise de documents écrits contenant leurs données personnelles car, au moment de la renonciation, ils ne connaissaient pas l'essentiel de l'information, objet de leur droit d'accès. En effet, dans ce cas précis, ils ignoraient alors que la banque communiquerait leurs données aux autorités américaines.

La charge de travail occasionnée à l'employeur pour délivrer les documents ne constitue pas un motif de refus[92] mais peut engendrer des frais (voir *infra*).

Dans certains cas exceptionnels, la communication écrite peut cependant être refusée, par exemple, lorsque les données n'ont pas été conservées sur papier ou ne sont pas imprimables (tels des enregistrements audio)[93].

Une consultation sur place peut remplacer une communication écrite si l'employé y consent[94]. La présence d'un avocat devrait être tolérée lors de la consultation si les documents consultables sont identiques à ceux que l'employeur aurait communiqués sous la forme écrite, ce qui devrait être le cas en pratique.

L'employeur a également la possibilité de prévoir la communication par voie électronique (art. 1 al. 2 OLPD), notamment dans un règlement d'entreprise.

Enfin, avec le consentement de l'employé, les données peuvent également être communiquées oralement (art. 1 al. 3 OLPD).

---

89 ATF 141 III 119, c. 7.6.2 ; jugement de l'Arbeitsgericht de Zürich CG120124 du 14 octobre 2013 confirmé par l'Obergericht dans LB130059 du 28 février, publié *in* : Entscheide des Arbeitsgerichtes Zürich 2013.

90 Sur ce point voir aussi l'arrêt de la Chambre civile de la Cour de justice genevoise ACJC/881/2014 du 16 juillet 2014, c. 6.1.

91 A teneur de l'article 8 al. 6 LPD, nul ne peut renoncer par avance au droit d'accès.

92 ATF 141 III 119, c. 8.1 ; 125 II 321, c. 3b ; 123 II 534, c. 3c ; arrêt de la Cour de justice genevoise ACJC/881/2014 du 16 juillet 2014, c. 6.1 et les jurisprudences citées.

93 MEIER, N 1078, p. 391.

94 ATF 123 II 534, c. 3c, *in* : JdT 1999 I 193.

b) Frais

En règle générale, l'employeur fournit gratuitement les renseignements requis (art. 8 al. 5 LPD).

Toutefois, une participation équitable aux frais peut exceptionnellement être demandée lorsque :

– les renseignements désirés ont déjà été communiqués au requérant dans les douze mois précédant la demande, et que ce dernier ne peut justifier d'un intérêt légitime, telle la modification non annoncée des données le concernant ;
– la communication des renseignements demandés occasionne un volume de travail considérable (art. 2 al. 1 OLPD).

Le montant prélevé s'élève à 300 francs au maximum. Le requérant est préalablement informé du montant et peut retirer sa requête dans les dix jours (art. 2 al. 2 OLPD).

2. Requête rejetée

Lorsque l'employeur refuse de fournir, restreint ou ajourne les renseignements, il doit en indiquer le motif dans les 30 jours suivant la réception de la demande (art. 9 al. 5 LPD et art. 1 al. 4 OLPD).

En cas de refus non justifié ou de renseignements incomplets ou inexacts, l'employé dispose des actions judiciaires prévues à l'article 15 LPD. Nous ne les décrirons cependant pas ici puisque celles-ci font l'objet d'une contribution approfondie dans le présent ouvrage[95].

IV. Conclusion

En théorie, le droit d'accès est conçu comme la clé de voûte de la protection des données.

Or, en pratique, nous constatons que ce droit démontre une portée plus limitée s'agissant du dossier personnel car le contenu de celui-ci dépend de la volonté de l'employeur.

Aussi, dans les situations conflictuelles, lorsque certaines données constituent un enjeu stratégique, il nous semble illusoire d'admettre qu'un employeur communique à son employé l'intégralité de ses données y compris celles dont ce dernier n'a pas connaissance, sans effectuer un tri préalable.

---

[95] A ce sujet, voir la contribution de Me AURÉLIEN WITZIG dans le présent ouvrage, pp. 29 ss.

En revanche, le droit d'accès présente un avantage certain lorsque l'employé souhaite obtenir l'accès à des documents déterminés comportant ses données, puisque, comme nous l'avons vu, dans la majorité des cas, les restrictions au droit d'accès peuvent être levées, notamment grâce au caviardage.

Partant, si le droit d'accès tel que prévu par la loi actuelle ne peut être envisagé comme un moyen de contrôle absolu sur les données personnelles, il peut s'avérer utile par exemple dans le but de contrôler l'exactitude de données en vue d'une procédure judiciaire.

L'avant-projet de la loi sur la protection des données devrait améliorer l'exercice de ce droit notamment en clarifiant et simplifiant certaines notions (p. ex. celles de fichier et profilage) mais aussi en renforçant les contrôles et les sanctions pénales[96].

Dès lors, véritable paradoxe, le droit d'accès donne tout son sens à l'adage populaire « savoir c'est pouvoir ».

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.

ATMANI MEHDI, Comment les « big data » façonnent l'employé moderne, *in* : Le Temps, 12 septembre 2013 Genève, disponible en ligne sur : http://www.letemps.ch/economie/2013/09/12/big-data-faconnent-employe-modele.

AUBERT GABRIEL, La communication aux autorités américaines, par des banques, de données personnelles sur leurs employés : aspects de droit du travail, *in* : RSDA 2013, pp. 40-48.

CARRANZA CARLOS JAÏCO/MICOTTI SÉBASTIEN, Whistleblowing : Perspectives en droit suisse, Genève 2014.

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

CUKIER KENNETH/MAYER-SCHÖNBERGER VIKTOR, Big Data : A Revolution That Will Transform How We Live, Work, and Think, New York 2014.

DUNAND JEAN-PHILIPPE, Commentaire de l'art. 328b CO, *in* : Jean-Philippe Dunand/Pascal Mahon (éds.), Commentaire du contrat de travail, Berne 2013.

FLÜCKIGER ALEXANDRE, L'autodétermination en matière de données personnelles : un droit (plus si) fondamental à l'ère digitale ou un nouveau droit de propriété ?, *in* : PJA 2013, pp. 837-864.

HUSI-STÄMPFLI SANDRA, Einschränkung des Auskunftsrechts, art. 9 DSG, *in* : Bruno Baeriswyl/Kurt Pärli (éds.), Datenschutzgesetz (DSG) - Handkommentar, Berne 2015.

[96] Rapport explicatif, p. 20.

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

MEYER BARBARA, Fragen und Antworten rund ums Personaldossier, *in* : L'expert-comptable suisse, ST 5/15, pp. 350-354.

MONNIER GILLES, Le droit d'accès aux données personnelles traitées par un média, Berne 1999.

OFFICE FÉDÉRAL DE LA JUSTICE, Rapport explicatif concernant l'avant-projet de loi fédérale sur la révision totale de la loi sur la protection des données et sur la modification d'autres lois fédérales du 21 décembre 2016 (cité : Rapport explicatif).

PAGE GÉRALD, Le droit d'accès aux données personnelles, *in* : Nicolas Gillard (éd.), La nouvelle loi fédérale sur la protection des données, Bulletin CEDIDAC nº 28, pp. 113-141.

PAGE GÉRALD, Le droit d'accès dans la Jurisprudence de la Commission fédérale de la protection des données, *in* : ZBI 108/2007, PP. 380 ss (cité PAGE, ZBI).

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

RUBIN BEAT, Auskunftsrecht, art. 8 DSG, *in* : Bruno Baeriswyl/Kurt Pärli (éds.), Datenschutzgesetz (DSG) - Handkommentar, Berne 2015.

RUDOLPH ROGER, Das Recht des Arbeitnehmers auf Einsicht in sein Personaldossier, *in* : PJA 2014, pp. 1672-1683.

STEINAUER PAUL-HENRI/FOUNTOULAKIS CHRISTIANA, Droit des personnes physiques et de la protection de l'adulte, Berne 2014.

STREIFF ULLIN/VON KAENEL ADRIAN/RUDOLPH ROGER, Arbeitsvertrag – Praxiskommentar zu art. 319-362 OR, 7e éd., Zurich/Bâle/Genève 2012.

WYLER REMY/HEINZER BORIS, Droit du travail, 3e édition, Berne 2014.

ESTELLE MATHIS-ZWYGART*

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

Sommaire

		Page
I.	Introduction	310
II.	Cadre légal	310
	A. Art. 328b CO	310
	1. Contexte	310
	a) Régime général de la protection de la personnalité	310
	b) Genèse de l'article 328b CO	311
	2. Champ d'application	311
	B. Art. 26 OLT 3	312
	1. Alinéa 1	313
	2. Alinéa 2	314
III.	Jurisprudence fédérale	314
	A. La surveillance par GPS	315
	1. ATF 130 II 425	315
	2. Arrêt du TF 2C_116/2011 du 29 août 2011	315
	B. La vidéosurveillance	316
	1. Arrêt du TF 6B_536/2009 du 12 novembre 2009	316
	2. ATF 138 V 125 et arrêt du TF 9C_785/2010 du 10 juin 2011	317
	C. La surveillance par logiciel espion	318
IV.	Quelques arrêts cantonaux	318
	A. Jura et Neuchâtel	318
	1. Jura	318
	2. Neuchâtel	319
	B. Valais	319
	C. Vaud	320
	1. Webcams dans une nurserie	320
	2. Logiciel espion de dernière génération	321
	D. Genève	322
	1. Consultation de sites pornographiques	322
	2. Transmission de données aux autorités américaines	322
V.	Synthèse	322
Bibliographie		323

* Je souhaite remercier chaleureusement ma collègue, Roxane Schaller, pour sa précieuse relecture.

I. Introduction

Déjà en 1988, deux problématiques s'affrontaient : l'évolution de la technologie dans de nombreux domaines et la protection de la personnalité des travailleurs. *« L'objectivité des décisions relatives au personnel, de même que la protection de la personnalité des employés ont tout à gagner de la rationalisation de la gestion du personnel au moyen des méthodes modernes de traitement des données ; ces méthodes sophistiquées n'ont cependant pas que des effets positifs : elles sont de nature à révéler presque toutes les facettes de la personnalité d'un employé, transparence que ne justifient en aucun cas les besoins réels de l'entreprise »*[1]. Le code civil et la loi sur le travail sont muets s'agissant de la surveillance des travailleurs sur leur lieu de travail, seule l'OLT 3 prévoit des règles à ce sujet. Selon le Tribunal fédéral[2], il conviendrait de régler la question de la surveillance des travailleurs sur le lieu de travail dans une loi au sens formel. À l'heure où la surveillance est de mise dans la plupart des lieux publics, mais aussi dans de nombreux établissements privés tels que centres commerciaux, parkings, hôtels, restaurants, etc., la remarque émise par notre Haute Cour mérite réflexion. La présente contribution présentera tout d'abord le cadre légal dans lequel s'inscrit la surveillance des travailleurs, puis la jurisprudence du Tribunal fédéral et différents arrêts cantonaux rendus dans ce domaine.

II. Cadre légal

Il sera traité de la surveillance des travailleurs uniquement sous l'angle de l'art. 328b CO (point **A.**) et de l'art. 26 OLT 3 (point. **B.**), tous deux en vigueur depuis 1993.

A. Art. 328b CO

1. Contexte

a) Régime général de la protection de la personnalité

Le régime général de la protection de la personnalité des travailleurs est prévu par l'art. 328 CO. L'employeur doit, dans les rapports de travail, protéger et respecter la personnalité de l'employé. Cette disposition prévoit une obligation générale d'assistance de l'employeur vis-à-vis de ses employés, contrepartie du devoir de fidélité imposé à l'employé par l'art. 321a CO. L'employeur doit s'abstenir de toute atteinte à la

1 Message LPD, FF 1988 II 421.

2 TF 6B_536/2009 du 12 novembre 2009, c. 3.3.2.

personnalité de l'employé qui n'est pas justifiée par le contrat de travail, mais il a également le devoir d'empêcher, dans le cadre des rapports de travail toujours, que des supérieurs hiérarchiques, des collaborateurs ou des tiers ne portent atteinte à la personnalité de l'employé.

b) Genèse de l'art. 328b CO

L'art. 328b CO a été introduit par le ch. 2 de l'annexe à la loi fédérale du 19 juin 1992 sur la protection des données (abrégée : LPD) et entré en vigueur le 1er juillet 1993. L'art. 328b CO prévoit que 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 LPD sont applicables.

L'introduction de l'art. 328b dans le CO avait pour but de protéger la personnalité du travailleur au moyen d'une disposition de protection des données spécifique[3]. Il a également été jugé nécessaire d'étendre la portée de l'art. 362 du CO en complétant la liste des dispositions du code auxquelles il ne peut être dérogé au détriment du travailleur[4]. Ces compléments apportés à la législation sur le contrat de travail ont été qualifiés d'indispensables car le rapport de travail, plus que n'importe quel autre rapport juridique, donne lieu à la collecte et au traitement de données personnelles de toute nature et pendant une longue durée[5]. Il se justifiait en conséquence d'accorder une protection particulière au travailleur, d'autant plus que celui-ci dépend en fait et en droit de son employeur[6]. Enfin, le principe général de la proportionnalité posé à l'art. 4 al. 3 LPD a été repris[7].

2. Champ d'application

Concernant la portée de l'art. 328b CO – controversée au sein de la doctrine – il est opportun de suivre l'avis du Tribunal fédéral d'après lequel les données personnelles couvertes par l'art. 328b CO bénéficient de la présomption légale qu'elles ne portent pas atteinte à la personnalité du travailleur[8]. Quant au champ d'application temporel de l'art. 328b CO, il est admis que dans certaines limites, le devoir de protection de la personnalité des travailleurs s'applique avant la conclusion du contrat et après la fin de celui-ci[9]. Le Tribunal fédéral a admis que les droits et obligations découlant des art. 328 et

3 Message LPD, FF 1988 II 421.
4 Message LPD, FF 1988 II 421.
5 Message LPD, FF 1988 II 421.
6 Message LPD, FF 1988 II 421.
7 Message LPD, FF 1988 II 421.
8 ATF 130 II 425, c. 3.3.
9 DUNAND, N 5 *ad* art. 328b CO et les références citées.

328b CO s'appliquent déjà au stade des pourparlers contractuels[10] et que la protection de l'art. 328b CO s'exerce non seulement pendant les rapports de travail, mais également après la fin de ceux-ci, sans limitation de temps[11].

Le Tribunal fédéral a précisé que l'employeur ne peut pas surveiller de façon générale ou systématique le comportement des travailleurs sous prétexte de récolter des données dont le traitement serait permis par l'art. 328b CO[12]. Il doit en particulier respecter la personnalité des travailleurs concernés, au sens de l'art. 328 CO, et observer les principes généraux du droit, en particulier ceux de la bonne foi et de la proportionnalité. Seules sont admissibles les mesures de surveillance objectivement justifiées qui satisfont un intérêt prépondérant de l'employeur. Entre plusieurs mesures possibles, ce dernier choisira la moins intrusive.

Comme déjà mentionné, il ne peut en aucun cas être dérogé à l'art. 328b CO au détriment de l'employé, même si ce dernier y consent (art. 362 CO).

B. Art. 26 OLT 3

La protection de la santé des travailleurs est consacrée par l'art. 6 de la Loi fédérale sur le travail dans l'industrie, l'artisanat et le commerce du 13 mars 1964 (abrégée : LTr). L'art. 6 LTr vise non seulement à protéger la santé physique et psychique des travailleurs, mais aussi leur *intégrité personnelle* (al. 1 *in fine*), à savoir leur personnalité au sens des art. 328ss CO. L'art. 6 al. 4 LTr prévoit que « *les mesures de protection de la santé qui doivent être prises dans les entreprises sont déterminées par voie d'ordonnance* ». C'est en vertu de cette délégation que le Conseil fédéral a adopté l'ordonnance 3 relative à la Loi sur le travail (abrégée : OLT 3) le 18 août 1993 qui est entrée en vigueur le 1er octobre de la même année. L'OLT 3 détermine les mesures de protection de la santé qui doivent être prises dans toutes les entreprises soumises à la loi (art. 1 OLT 3). Pour rappel, la LTr s'applique à toutes les entreprises publiques et privées (art. 1 LTr), sous réserve des art. 2 à 4 LTr qui prévoient les exceptions quant aux entreprises (art. 2 LTr), aux personnes (art. 3 LTr) et le cas particulier des entreprises familiales (art. 4 LTr).

Même si leurs effets exacts sur la santé ne sont pas définitivement connus, il est généralement admis que les systèmes de surveillance induisent le plus souvent chez les personnes observées des sentiments négatifs et détériore le climat général de l'entreprise et que, par conséquent, ils nuisent au bien-être, à la santé psychique et, finalement, à la

10 TF 2C_103/2008 du 30 juin 2008, c. 6.2.
11 ATF 131 V 298, c. 6.1.
12 ATF 130 II 425, c. 3.3.

capacité de rendement des travailleurs[13]. C'est d'ailleurs en vue de protéger la santé psychique des travailleurs que le Conseil fédéral a, semble-t-il, donné suite à la motion parlementaire à l'origine de l'art. 26 OLT 3[14].

Précisément, l'art. 26 al. 1 OLT 3 prévoit qu'il est interdit d'utiliser des systèmes de surveillance ou de contrôle destinés à surveiller le comportement des travailleurs à leur poste de travail. L'al. 2 précise que lorsque des systèmes de surveillance ou de contrôles sont nécessaires pour d'autres raisons, ils doivent notamment être conçus et disposés de façon à ne pas porter atteinte à la santé et à la liberté de mouvement des travailleurs. L'art. 26 OLT 3 a pour but de protéger la santé, la liberté de mouvement et la personnalité des travailleurs en interdisant les systèmes de surveillance ou de contrôle destinés à surveiller le comportement des travailleurs.

1. Alinéa 1

Par système de surveillance ou de contrôle, il faut entendre « *tous les systèmes techniques (optiques, acoustiques, électroniques, etc.) qui permettent d'enregistrer une ou plusieurs activités ou le comportement des travailleurs* »[15]. À préciser encore que « *la surveillance du comportement des travailleurs comprend toute surveillance permettant de vérifier, en permanence (de façon ininterrompue) ou non (par des contrôles périodiques sur de brefs espaces de temps ou par des contrôles par échantillons), certaines activités des travailleurs de façon détaillée* »[16].

Comme exemples concrets de surveillance ou de contrôle, nous pouvons citer :[17]

- les équipements vidéo et les caméras qui filment et enregistrent ce que font les travailleurs ;
- les microphones ou interphones ou tout autre support audio permettant d'enregistrer ce que disent les travailleurs ;
- les systèmes de localisation que l'on pourrait avoir dans un véhicule de service ;
- les programmes informatiques permettant de connaître les activités des travailleurs à l'ordinateur ;
- les systèmes et réseaux informatiques ;
- les centrales et réseaux téléphoniques ainsi que les systèmes d'écoute téléphonique ;

13 ATF 130 II 425, c. 3.3 et les nombreuses références citées.
14 ATF 130 II 425, c. 3.3 et les nombreuses références citées.
15 SECO, Commentaire de l'OLT 3, p. 326-2.
16 SECO, Commentaire de l'OLT 3, p. 326-2.
17 SECO, Commentaire de l'OLT 3, p. 326-2.

– les appareils permettant de faxer et/ou photocopier des documents ;
– Internet.

Par contre, ne sont pas considérés comme des systèmes de surveillance ou de contrôle :[18]

– les badges ou cartes électroniques pour pouvoir entrer dans l'entreprise ;
– le système de « timbrage » permettant d'enregistrer l'heure d'entrée dans l'entreprise et de sortie ;
– les systèmes électroniques de contrôle de qualité permettant de comptabiliser quotidiennement l'ensemble de la production d'une installation.

2. Alinéa 2

Dans la mesure où ils excluent la surveillance du comportement des travailleurs, des systèmes de surveillance et de contrôle peuvent être disposés à tous les endroits stratégiques pour l'entreprise et où les travailleurs accèdent rarement tels que :[19]

– l'extérieur des bâtiments, les parkings extérieurs et souterrains ;
– les accès, entrées et passages ;
– la salle des coffres ;
– les lieux intérieurs ou extérieurs où se situent les machines et installations dangereuses, les dépôts de produits dangereux.

À préciser encore que les systèmes d'enregistrement du temps de travail, les contrôles d'accès à l'entreprise, les systèmes de suivi des mandats, etc. doivent être utilisés de telle manière qu'on ne puisse pas tirer de conclusions sur le comportement des travailleurs[20].

III. Jurisprudence fédérale

Cela fait bientôt un quart de siècle que le cadre légal est posé, mais seulement une dizaine d'années que l'activité jurisprudentielle bat son plein. Nous passerons d'abord en revue la jurisprudence rendue par le Tribunal fédéral (chapitre **III.**), chapitre que nous avons divisé selon le système de surveillance qui est traité (point **A.** La surveillance par GPS, point **B.** La vidéosurveillance, point **C.** La surveillance par logiciel espion), ce qui permet de comparer ce qui est comparable. Ensuite, nous examinerons quelques arrêts cantonaux

[18] SECO, Commentaire de l'OLT 3, p. 326-2.
[19] SECO, Commentaire de l'OLT 3, p. 326-2 et 3.
[20] SECO, Commentaire de l'OLT 3, p. 326-3.

(chapitre **IV.**) – parfois rendus avant la mise en place du cadre légal – que nous avons jugés intéressants pour leur état de fait.

A. La surveillance par GPS

1. ATF 130 II 425

Dans un arrêt concernant la conformité au droit de l'installation d'un système GPS sur des véhicules d'entreprise dont des employés se servaient régulièrement à des fins professionnelles, le Tribunal fédéral n'a pas exclu que des mesures de surveillance objectivement justifiées, qui satisfont un intérêt prépondérant de l'employeur et qui sont proportionnées, soient admissibles[21]. L'affaire du GPS a permis de poser les premiers principes, à savoir que sont interdits les systèmes de surveillance ou de contrôle qui sont destinés à surveiller le comportement des employés à leur poste de travail, mais non ceux qui sont nécessaires pour d'autres raisons, tels que la prévention des accidents, la protection des personnes et des biens ou le contrôle de la qualité des prestations. À préciser encore que le système de surveillance choisi doit être proportionné au but poursuivi et les travailleurs informés au préalable de son utilisation[22]. À ce titre, notre Haute Cour a jugé que des motifs tenant à l'organisation ou à la planification du travail pouvaient justifier la mise en place d'un système GPS. Pour les entreprises de taxi ou de transport routier, il est important que l'employeur ait la possibilité de localiser en tout temps et aussi vite que possible la position de chacun des véhicules en service afin de rationaliser le travail et d'améliorer la qualité des prestations offertes aux clients[23]. L'employeur est également habilité, sous réserve d'en avoir préalablement informé les travailleurs, à prendre des mesures appropriées destinées à contrôler leur travail, en particulier la qualité de leurs prestations et leur rendement[24].

2. Arrêt du TF 2C_116/2011 du 29 août 2011

Dans un arrêt plus récent, concernant des exploitants de taxis, le Tribunal fédéral a repris les principes dégagés dans l'arrêt précédent[25]. Il a admis que la localisation des taxis par GPS est une mesure proportionnée compte tenu des objectifs poursuivis par la loi ; à l'intérêt privé des chauffeurs de taxi à ce que leurs déplacements ne soient pas traçables par la société concessionnaire s'oppose l'intérêt public à pouvoir joindre et coordonner rapidement les chauffeurs de taxi qui se trouvent à proximité immédiate d'un usager et à

21 ATF 130 II 425, c. 3.3.
22 ATF 130 II 425, c. 4.2 à 4.4.
23 ATF 130 II 425, c. 4.2 ; cf. aussi son c. 5.4.1.
24 ATF 130 II 425, c. 4.2.
25 TF 2C_116/2011 du 29 août 2011, *in* : SJ 2011 I 405, c. 8.

vérifier que ceux-ci observent les conditions minimales inhérentes au quasi-service public. En outre, le caractère incisif de la mesure de surveillance doit être relativisé, dès lors que la localisation par GPS se confine aux heures d'activités professionnelles effectives, le chauffeur de taxi étant libre de le débrancher en dehors de celles-ci, à tout moment. Le chauffeur subit de plus un contrôle médiat, qui porte non pas sur sa personne mais sur le mouvement des véhicules utilisés et qui n'est pas de nature audiovisuelle, réputée plus intrusive[26].

B. La vidéosurveillance

1. Arrêt du TF 6B_536/2009 du 12 novembre 2009

Dans cet arrêt de 2009, le Tribunal fédéral a estimé qu'un système de contrôle auquel les salariés n'étaient soumis que de manière sporadique n'était pas contraire à l'art. 26 OLT 3. L'état de fait était le suivant. L'employeur a porté plainte pour vol contre l'une de ses employées qui avait été filmée, par une caméra installée dans le local de caisse, à l'insu des collaborateurs, en train de prélever des billets de banque, posant ceux-ci sur la tablette, recouvrant celle-ci d'une feuille de papier, sortant du local avec la tablette et revenant quarante secondes plus tard sans l'argent pour broyer la feuille de papier qui recouvrait les billets de banque. Le Tribunal fédéral a estimé que la surveillance vidéo du local de caisse ne contrevenait pas à l'art. 26 OLT 3 pour les raisons suivantes. Tout d'abord, l'art. 26 al. 1 OLT 3 doit être interprété restrictivement en ce sens que les systèmes de contrôle et de surveillance destinés à surveiller le comportement des travailleurs sur le lieu de travail sont interdits dans la mesure où ils sont susceptibles de porter atteinte à la santé ou au bien-être des travailleurs. C'est seulement à cette condition que l'interdiction de la surveillance constitue une mesure pour la protection de la santé au sens de l'art. 6 al. 4 LTr[27]. Ensuite, le but de la mesure de surveillance n'est qu'un critère parmi d'autres (fréquence, durée, etc. de la surveillance) qui peuvent être pertinents au regard de la protection de la santé. Un système de surveillance peut donc être permis même s'il sert (principalement) à la surveillance ciblée du comportement des travailleurs sur le lieu de travail, si les travailleurs ne sont enregistrés que sporadiquement et pendant peu de temps, à certaines occasions particulières, par le système de surveillance[28]. En l'espèce, les travailleurs ne se trouvaient que sporadiquement et pendant de courtes durées dans le local de caisse, soit lorsqu'ils s'y rendaient pour y déposer ou pour y prélever des espèces. Le comportement des travailleurs sur le lieu de travail n'était pas surveillé sur une longue période par la surveillance vidéo dans le local de caisse, qui enregistrait principalement la caisse, près de laquelle les

[26] Arrêt de la CourEDH *Üzun c. Allemagne,* du 2 septembre 2010, requête n° 35623/05, par. 52.
[27] TF 6B_536/2009 du 12 novembre 2009, c. 3.6.1.
[28] TF 6B_536/2009 du 12 novembre 2009, c. 3.6.2.

travailleurs se trouvaient sporadiquement et pendant un moment bref. Une telle surveillance vidéo n'est pas de nature à porter atteinte à la santé et au bien-être des travailleurs. Vu son manque de pertinence sous l'angle de la santé et du bien-être des travailleurs, elle n'est pas interdite par l'art. 26 al. 1 OLT 3, selon l'interprétation restrictive qui s'en impose[29]. Le Tribunal fédéral a enfin examiné la question de savoir si la surveillance des travailleurs sur le lieu de travail, par exemple par des caméras vidéo, peut, selon les circonstances concrètes, également violer la personnalité des travailleurs au sens des art. 28 CC, 328 CO et 328b CO et/ou enfreindre les dispositions de la LPD. La surveillance vidéo du local de caisse n'a pas exclusivement pour but la surveillance du personnel, mais également la prévention d'infractions pénales par des tiers. Des sommes en espèces d'un montant considérable peuvent se trouver dans le local de caisse d'un magasin de montres et de joaillerie, si bien que le propriétaire a un intérêt considérable à la surveillance. Pendant une journée de travail, les travailleurs ne sont enregistrés que sporadiquement et pendant de courtes durées par la surveillance vidéo dans le local de caisse. Dans les circonstances du cas d'espèce, la personnalité de l'employée n'a pas été atteinte de manière illicite au sens des art. 28 CC, 328 et 328b CO, respectivement 12 LPD. Ce constat demeure valable même si l'employée, non seulement ne savait pas qu'une caméra vidéo pouvait être installée dans le local de caisse et fonctionner pendant les heures d'ouverture du commerce, mais encore ne comptait pas avec cette possibilité[30].

2. ATF 138 V 125 et arrêt du TF 9C_785/2010 du 10 juin 2011

En 2011, le Tribunal fédéral a eu deux fois l'occasion de se pencher sur de la vidéosurveillance[31]. Les deux arrêts, dont l'état de fait est similaire, ont rapport avec l'admissibilité du moyen de preuve dans l'examen de la réduction des prestations par des assureurs sociaux. Notre Haute Cour a précisé le principe en admettant un système de vidéosurveillance d'une caisse enregistreuse limité à la caisse et aux mains des utilisateurs, à condition que le système ne soit pas permanent, mais installé en cas de soupçons concrets de vols de la part de certains salariés. Comme l'objectif était d'empêcher les détournements dans la caisse et des déprédations, il n'était pas nécessaire d'aviser le personnel visé. Le Tribunal fédéral a rappelé que des systèmes de surveillance destinés à assurer la sécurité, l'organisation au travail ou la qualité du travail sont admissibles selon l'art. 26 OLT 3. La vidéosurveillance d'une caisse est un moyen approprié pour empêcher les vols ou les découvrir, à condition que les employés ne soient pas surveillés de manière large et permanente, mais uniquement pendant des périodes limitées de temps, voire en présence de soupçons concrets afin que l'atteinte à leur personnalité ne soit pas sévère et que le principe de la proportionnalité soit respecté.

---

29 TF 6B_536/2009 du 12 novembre 2009, c. 3.6.3.

30 TF 6B_536/2009 du 12 novembre 2009, c. 7.

31 ATF 138 V 125 et TF 9C_785/2010 du 10 juin 2011, *in* : JdT 2013 II 187.

C. La surveillance par logiciel espion

Le Tribunal fédéral a dû se prononcer sur l'admissibilité d'un logiciel espion destiné à vérifier si des ressources informatiques étaient détournées[32]. Il a décidé que la mise en place dissimulée d'un système de surveillance automatique qui récolte toutes les données relatives à l'utilisation d'un ordinateur, à savoir un logiciel espion, et qui permet à l'employeur de relever toutes les activités effectuées par l'employé depuis son poste de travail personnel (pages web consultées, messagerie privée, etc.), en obtenant également des captures régulières d'écran, permettant ainsi à l'employeur de prendre connaissance d'informations à caractère confidentiel de type familial (courriel de la femme de l'employé sur des questions délicates strictement privées et curriculum vitae du fils de l'employé), de type bancaire (opérations bancaires avec indication des numéros de compte, des paiements et en partie des bénéficiaires des paiements) ou institutionnel (liées à l'activité politique de l'employé) n'est pas admissible. Même si l'employeur a des soupçons, un tel logiciel a essentiellement pour but de surveiller l'employé à son insu et constitue une atteinte disproportionnée et trop intrusive, ne respectant pas l'art. 26 OLT 3. En effet, l'employeur aurait pu recourir à des moyens moins invasifs pour contrôler les abus de l'employé et y mettre fin, notamment en se conformant au Guide édicté par le Préposé fédéral à la protection des données. En conséquence, le Tribunal fédéral n'a pas admis les moyens de preuve recueillis illicitement pour justifier la décision de licencier avec effet immédiat cet employé de la fonction publique.

IV. Quelques arrêts cantonaux

A. Jura et Neuchâtel

1. Jura

Dans un arrêt rendu en 1989, le Tribunal cantonal du Jura a dû se prononcer sur la licéité de l'installation d'une caméra vidéo dans un atelier pour surveiller le fonctionnement de machines automatiques qui ne sont pas desservies par du personnel, en précisant qu'il était toutefois possible d'apercevoir un travailleur[33]. Le Tribunal cantonal du Jura a jugé cette mesure licite. Il a en revanche ajouté que si la caméra avait été orientée en permanence sur une place de travail où se trouvait un salarié, son installation aurait porté atteinte aux droits de la personnalité de ce dernier, et ce, même si la caméra n'était en général pas enclenchée et qu'elle ne visait pas la surveillance du personnel. Dans un tel cas, il y aurait eu une

[32] ATF 139 II 7, *in* : JdT 2013 II 187.

[33] Arrêt du Tribunal cantonal du Jura du 19 septembre 1989, *in* : SJ 1990 247.

atteinte à la personnalité du travailleur et l'employeur aurait pu se voir intimer l'ordre de mettre hors service la caméra. Il est important de noter que cet arrêt a été rendu avant l'entrée en vigueur des art. 328b CO et 26 OLT 3 et que le raisonnement n'a pas été rendu obsolète par la jurisprudence du Tribunal fédéral en matière de vidéosurveillance. Au contraire, cet arrêt de 1989 reste d'actualité.

2. Neuchâtel

Le Tribunal cantonal neuchâtelois a estimé que le fait que l'employeur place à l'insu du travailleur un émetteur de localisation GPS sur son véhicule de fonction – qu'il avait le droit d'utiliser à des fins privées – constituait, au vu notamment de la dissimulation de l'installation, une atteinte illégitime à la santé du travailleur[34]. Il est à noter que dans ce cas, contrairement à ceux traités par le Tribunal fédéral, il s'agissait d'un véhicule de fonction également utilisé dans le privé et qu'en plus l'installation du GPS avait été faite à l'insu de l'employé.

B. Valais

Le Tribunal cantonal valaisan a dû se pencher sur la surveillance de deux nettoyeuses chargées d'entretenir, entre 5h et 7h du matin du lundi au samedi, le premier étage du magasin qui les employait[35]. Au premier étage se situait le rayon des vêtements et des appareils. Grâce à la vidéosurveillance du magasin, il a été établi que les deux employées en question avaient dérobé quasi quotidiennement des sous-vêtements, habits, articles de maroquinerie et appareils dans les rayons du magasin. Lors de l'appel contre le jugement de première instance, l'une des deux employées a soutenu que la vidéosurveillance violait les art. 26 OLT 3, 4 à 7 LPD et 328 CO car elle visait à contrôler son comportement ainsi que celui de sa collègue et qu'elles n'avaient pas été informées de la mise en place de ces mesures. En référence à la jurisprudence du Tribunal fédéral[36], il a été décidé que la vidéosurveillance n'avait pas été mise en place principalement en vue de contrôler les nettoyeuses, mais prioritairement pour des motifs de sécurité, à savoir la prévention de vols durant les heures d'ouverture du magasin, mais également en dehors de ces horaires. Ensuite, les caméras étaient fixes de sorte que, si l'employée s'était contentée d'effectuer le travail confié, elle ne se serait trouvée dans le champ de celles-ci que de façon temporaire et passagère, ce qui ne saurait constituer une atteinte à sa santé. En outre, le fait d'ignorer l'existence du système de surveillance, alors même qu'il est notoire que les commerces y recourent depuis de nombreuses années, ne rendait pas celui-ci illicite. Enfin,

---

34 Arrêt du Tribunal cantonal neuchâtelois CHAC.2010.23 du 14 juin 2006.

35 Arrêt du Tribunal cantonal valaisan du 21 février 2014, *in* : RVJ 2015 p. 220.

36 TF 6B_536/2009 du 12 novembre 2009.

à l'instar des clients, l'employée devait tolérer d'être filmée car l'intérêt de l'employeur de prévenir, comme en l'espèce, des infractions pénales susceptibles de léser sa propriété, justifiait l'atteinte limitée à la personnalité des personnes filmées.

C. Vaud

1. Webcams dans une nurserie

Le Tribunal administratif vaudois a rendu une décision intéressante en 2005 sur la question de savoir si l'utilisation de webcams dans une nurserie respectait les art. 328 CO et 26 OLT 3[37]. Il est tout d'abord rappelé que la portée des art. 26 OLT 3 et 328 CO a été examinée par le Tribunal fédéral dans un arrêt du 13 juillet 2004 concernant notamment l'adéquation d'un système de contrôle par localisation satellite (GPS) par rapport au but visé et la nécessité du système pour l'employeur[38]. Le Tribunal administratif vaudois reprend les considérants du Tribunal fédéral en rappelant que même si leurs effets exacts sur la santé ne sont pas définitivement connus, il est généralement admis que les systèmes de surveillance induisent le plus souvent chez les personnes observées des sentiments négatifs et détériorent le climat général de l'entreprise et que, par conséquent, ils nuisent au bien-être, à la santé psychique et, finalement, à la capacité de rendement des travailleurs. En d'autres termes, un système de surveillance est interdit par l'art. 26 OLT 3 s'il vise uniquement ou essentiellement à surveiller le comportement comme tel des travailleurs. En revanche, son utilisation n'est pas prohibée si, bien qu'emportant objectivement un tel effet de surveillance, il est justifié par des raisons légitimes, tels que des impératifs de sécurité ou des motifs tenant à l'organisation ou à la planification du travail ou encore à la nature même des relations de travail. Encore faut-il cependant que le système de surveillance choisi apparaisse, au vu de l'ensemble des circonstances, comme un moyen proportionné au but poursuivi et que les travailleurs concernés aient préalablement été informés de son utilisation[39]. Dans le cas soumis au Tribunal administratif du canton de Vaud, le Service de la protection de la jeunesse, tout en admettant que le système de webcams envisagé n'était pas destiné en premier lieu à surveiller le comportement des membres de l'équipe éducatrice, a estimé néanmoins qu'il permettrait une telle surveillance et que cet élément suffit pour constituer une atteinte aux droits de la personnalité des employés. D'après l'avis de la propriétaire de la nurserie, le visionnement aurait au contraire un objectif purement pédagogique tendant à permettre aux parents de suivre pendant un temps limité chaque jour l'activité de leurs enfants au sein de leur groupe. De plus, les heures exactes de tournage seraient clairement connues

37 Arrêt du Tribunal administratif vaudois GE.2002.0088 du 28 juin 2005.
38 ATF 130 II 425.
39 ATF 130 II 425.

des collaborateurs puisqu'elles seraient fixées selon un programme communiqué à tous les intéressés (éducatrices/parents) au début de chaque mois (cf. règlement). Même si le Tribunal administratif vaudois était prêt à admettre que le but premier des webcams n'était pas de surveiller les éducatrices, il n'en demeure pas moins que les images enregistrées permettraient d'exercer – de fait – un contrôle sur la manière dont les éducatrices effectuent leur travail. En outre, le Tribunal administratif vaudois a estimé qu'aucune raison légitime (motif de sécurité ou lié à l'organisation du travail notamment) n'imposait de recourir au système envisagé. L'éventuel intérêt que pouvait représenter pour les parents la possibilité de voir leurs enfants via Internet quelques minutes par jour ne constituait en aucun cas un motif suffisant, d'autant plus que, comme exposé ci-dessus, les webcams étaient de nature à porter une atteinte, réelle quant à elle, aux intérêts des enfants. Enfin, le Préposé à la protection des données a également confirmé que l'utilisation de systèmes de surveillance et de contrôle qui surveillent le comportement des employés à leur place de travail n'était pas autorisée, sauf s'ils étaient nécessaires pour d'autres raisons. En conclusion, le Tribunal administratif vaudois a constaté que l'utilisation de webcams dans la nurserie ne respectait ni l'art. 26 OLT 3 ni l'art. 328 CO.

2. Logiciel espion de dernière génération

Une deuxième affaire vaudoise, traitée elle par la Cour des assurances sociales[40], concerne l'installation d'un logiciel espion. L'employeur, une société active dans la prestation de services, conseils et développements dans le domaine de l'informatique, avait placé sur le poste de travail de l'un de ses employés un logiciel de la dernière génération qui « *permet en particulier de surveiller l'ensemble des activités exécutées, en stockant localement les données capturées ou les envoyant discrètement (par exemple par courriel caché, ou avec une connexion à distance) à l'attaquant. Ce dernier peut ainsi voir toutes les pages Internet visitées, épier les contenus de tous les courriels envoyés et reçus ou encore capturer la saisie (keylogger) de l'utilisateur, donc aussi les mots de passe qu'il a introduits* ». L'employé a découvert l'installation du logiciel espion et a démissionné aux motifs qu'un tel logiciel est contraire à la LPD et que l'employeur ne l'a jamais informé par oral ou par écrit de l'installation de ce logiciel, ce qui constitue une faute de l'employeur au sens de l'art. 7a LPD. La Cour des assurances sociales a estimé qu'il était établi que l'employeur avait installé un logiciel espion sur le poste de travail de son employé, sans l'en informer, et qu'au regard des impressions de capture d'écran produites par l'employé, ce logiciel permettait effectivement à l'employeur de prendre connaissance de toute l'activité du recourant sur son ordinateur (consultation des sites visités, frappes sur le clavier, mots de passe, etc.), ce qui constitue une violation grave des art. 328 al. 1 CO et 26 OLT 3.

[40] Arrêt de la Cour des assurances sociales ACH 140/10 du 31 mai 2012.

D. Genève

1. Consultation de sites pornographiques

La Cour de justice a dû se prononcer sur le cas d'un employé de la Ville de Genève, soupçonné de consulter des sites pornographiques sur son lieu de travail[41]. L'employé avait signé en 2003 un engagement destiné à respecter la directive relative à l'utilisation des systèmes d'information et de communication. L'employé certifiait en avoir pris connaissance et prenait bonne note du fait qu'en cas de soupçon de violation de ladite directive, une surveillance individualisée et la consultation de messages ou fichiers douteux pouvaient être ordonnées conformément à l'art. 21 de cette directive. Lorsque la Ville de Genève a éprouvé des soupçons de violation de la directive par son employé, elle a appliqué l'art. 21 et mis en place une première surveillance qui a confirmé la consultation de sites pornographiques par l'employé. Une seconde surveillance a eu lieu pour reconstituer les fichiers effacés. L'art. 26 OLT 3 a été respecté car la Ville de Genève a agi sur la base d'une directive connue de son employé, au surplus en deux temps, respectant ainsi la jurisprudence relative à l'art. 26 OLT 3 et le principe de la proportionnalité.

2. Transmission de données aux autorités américaines

La Cour de justice a dû se prononcer sur le cas d'un employeur, un établissement bancaire, qui a communiqué aux autorités américaines, hors d'une procédure d'entraide internationale, des documents contenant des données de l'une de ses *Relationship Manager*, soit des informations l'identifiant ou permettant de l'identifier[42]. La Cour de Justice a qualifié cette communication comme contraire à l'art. 328b CO dans la mesure où le moyen tiré de l'art. 6 al. 2 let. d LPD avait été rejeté et parce que l'établissement bancaire ne s'était pas prévalu d'un autre motif justificatif prévu à l'article 6 al. 2 LPD.

V. Synthèse

Quelques remarques peuvent être faites en cette fin de contribution. Comme nous l'avons vu au travers des différents arrêts parcourus, la protection offerte aux travailleurs en droit privé est équivalente à celle offerte en droit public : il suffit de s'adapter aux moyens et voies de droit propres à chaque droit pour faire respecter les règles sur la protection de la personnalité des travailleurs[43]. Cette jurisprudence est cohérente et s'impose de manière

41 Arrêt de la Cour de Justice de Genève, chambre administrative, ATA/329/2013 du 28 mai 2013.

42 Arrêt de la Cour de Justice de Genève, chambre civile, ACJC/1529/2015 du 11 décembre 2015.

43 WYLER, pp. 187 ss.

équilibrée entre la préservation des intérêts légitimes de l'employeur et le respect de la personnalité du travailleur[44]. Les principes qui ont été dégagés au fil des années par le Tribunal fédéral, et par les instances cantonales dans une certaine mesure, peuvent s'appliquer à tous les cas de surveillance, tout en laissant une marge d'appréciation suffisamment grande au juge appelé à se prononcer en fonction de l'état de fait et du système de surveillance utilisé. Au vu des moyens technologiques que nous avons aujourd'hui, les employés peuvent craindre d'être suivis, filmés et espionnés, mais ils peuvent aussi se rassurer car notre Haute Cour a défini de manière suffisamment précise les limites que les employeurs ne peuvent pas franchir en matière de surveillance.

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.

AUBERT CAROLE/RÉGINE DELLEY, Utilisation des réseaux sociaux par les travailleurs et les employeurs, *in* : Jean-Philippe Dunand/Pascal Mahon (éds.), Internet au travail, Genève/Zurich/Bâle 2014, pp. 131-162.

AUBERT GABRIEL, Commentaire des art. 319-362 CO, *in* : Luc Thévenoz/Franz Werro (éds.), Commentaire romand, Code des obligations I, 2e édition, Bâle 2012.

AUBRY GIRARDIN FLORENCE, La protection du salarié en droit public : incidences sur le droit privé du travail, *in* : Rémy Wyler/Anne Meier/Sylvain Marchand (éds.), Regards croisés sur le droit du travail : *Liber Amicorum* pour Gabriel Aubert, Genève 2015, pp. 27-39.

BRUNNER CHRISTIANE/BÜHLER JEAN-MICHEL/WAEBER JEAN-BERNARD/BRUCHEZ CHRISTIAN, Commentaire du contrat de travail, 3e édition, Lausanne 2004.

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

CONSEIL FÉDÉRAL, Message concernant la loi fédérale sur la protection des données (LPD) du 23 mars 1988, FF 1988 II 421 (cité : Message LPD).

COTTIER BERTIL, La protection des données, *in* : Julien Perrin (éd.), Internet au lieu de travail, Lausanne 2004, pp. 81-108.

DUNAND JEAN-PHILIPPE, L'usage de l'Internet sur le lieu de travail au vu de la jurisprudence récente du Tribunal fédéral, *in* : Julien Perrin (éd.), Internet au lieu de travail, Lausanne 2004, pp. 1-35.

DUNAND JEAN-PHILIPPE, Commentaire de l'art. 328b CO, *in* : Jean-Philippe Dunand/Pascal Mahon (éds.), Commentaire du contrat de travail, Berne 2013, pp. 317-355.

[44] WYLER, pp. 187 ss.

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.

GEISER THOMAS, Die Beaufsichtigung des Internetbenutzers im Arbeitsrecht, *in* : Medialex 2001/4, pp. 201-209.

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

METILLE SYLVAIN, La surveillance électronique des employés, *in* : Jean-Philippe Dunand/Pascal Mahon (éds.), Internet au travail, Genève/Zurich/Bâle 2014, pp. 99-128.

ORDOLLI GENEVIÈVE, Les systèmes de surveillance des travailleurs : aspects de droit individuel et collectif, *in* : Jean-Philippe Dunand/Pascal Mahon (éds.), Le droit décloisonné, interférences et interdépendances entre droit privé et droit public, Genève 2009, pp. 199-224.

ORDOLLI GENEVIÈVE, Intranet et internet dans les rapports collectifs de travail – Etude de droit suisse et de droit comparé, Genève 2013.

PRÉPOSÉ FÉDÉRAL À LA PROTECTION DES DONNÉES ET À LA TRANSPARENCE, Guide relatif à la surveillance de l'utilisation d'Internet et du courrier électronique au lieu de travail à l'attention de l'économie privée, Berne 2013 (cité : PFPDT, Guide relatif à la surveillance).

SECRÉTARIAT D'ETAT À L'ECONOMIE (SECO), Commentaire de l'ordonnance 3 relative à la loi sur le travail, état en mars 2013, Berne 2013 (cité : SECO, Commentaire de l'OLT 3).

SUBILIA OLIVIER/DUC JEAN-LUC, Droit du travail – Eléments de droit suisse, 2e édition, Lausanne 2010.

WYLER, RÉMY, Chronique de jurisprudence en droit du travail, *in* : JdT 2013 II 187.

WYLER RÉMY/HEINZER BORIS, Droit du travail, 3e édition, Berne 2014.

JEAN CHRISTOPHE SCHWAAB*

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

Sommaire

		Page
I.	Qu'est-ce que le « forced ranking »?	326
II.	Problèmes posés par le « forced ranking »	328
III.	Considérations juridiques	330
	A. Droit de l'employeur d'évaluer	330
	B. Droit des salariés face à l'évaluation	331
	C. Respect de la protection des données	333
	D. Discrimination de genre	333
	E. Risque de mobbing	334
	F. L'évaluateur	334
	G. L'évaluation par un évaluateur externe	335
	1. L'évaluation par les clients et les usagers	335
	2. L'évaluation secrète (clients mystères et achats tests)	336
	a) Les clients mystères	337
	b) Les achats tests	338
IV.	Conclusion : Les conditions de la licéité de l'évaluation	339
Bibliographie		340

La présente contribution traite d'une forme particulière d'évaluation, les évaluations « forcées » ou « forced ranking ». Elle se penche également sur la licéité de l'évaluation en général, ainsi que sur deux formes d'évaluations qui, numérisation de l'économie oblige, gagnent en importance : l'évaluation par les clients et les évaluations que l'employeur ou une institution externe mène en secret, dans le but d'évaluer la prestation du personnel ou le respect des lois (achats tests et clients mystères).

---

* La présente contribution est une version augmentée de l'article paru in Jusletter du 4 juillet 2016. Je remercie Jennifer Lygren, Denise Chervet et Luca Cirigliano pour leurs idées et relecture critique, les services du Parlement pour leur contribution à la documentation ainsi que les éditions Weblaw (éditeur de Jusletter).

I. Qu'est-ce que le « forced ranking »?

Le « forced ranking » (ou « forced distribution ») est une forme d'évaluation du personnel qui a pour but de classer les salariés en catégories (p. ex. : « bon », « moyen », « mauvais ») et qui fixe au départ un certain quota à atteindre pour ces différentes catégories (p. ex. selon une courbe de Gauss). Une variante consiste à une intervention de la hiérarchie *après* que les évaluations aient été faites, dans le but de corriger ses résultats, p. ex. s'il y a trop de « bons » ou pas assez de « mauvais ». Selon que l'on soit classé dans l'une des différentes catégories, cela peut avoir une influence sur le salaire (p. ex. annuité ou bonus), sur la carrière interne ou carrément sur la poursuite de la relation de travail si une mauvaise évaluation entraîne un licenciement ou si les résultats permettent la constitution d'une « réserve » d'employés pouvant être licenciés en cas de restructuration. Cela peut aussi avoir une influence sur le certificat de travail, et donc sur la suite de la carrière professionnelle auprès d'autres employeurs.

Cette méthode d'évaluation a été inventée dans les années 1980 par le directeur de General Electric (GE) Jack WELCH : il s'agissait de classer les collaborateurs en trois quotas de 20% « excellents » (à promouvoir), 70 % de « moyens » et 10% d'« insuffisants » (à licencier), dans le but d'augmenter la productivité et la motivation, car, grâce à cette méthode, « seuls les meilleurs restent à bord ». M. WELCH nommait malicieusement la courbe de Gauss ainsi obtenue « courbe de vitalité ». Cette méthode se résume parfois en « rank and yank » (classer et virer)[1]. On la trouve (ou la trouvait, à tout le moins sous forme de rumeurs) surtout dans des multinationales anglo-saxonnes (HP, Yahoo, IBM, General Electric, PepsiCo, Sun Microsystems, Caterpillar, Cisco Systems, EDS, Dow Chemical, Amazon, American Airlines), dans les grandes banques (UBS[2]), mais aussi dans certains services et administrations publics (administration fédérale, CFF). Selon certaines estimations, un quart des grandes entreprises étatsuniennes du classement « Fortune 500 » pratiqueraient cette méthode[3]. Un sondage mené au Royaume-Uni auprès de 562 dirigeants d'entreprise révèle que, si 77% des sondés pensent que le « forced ranking » peut mener à des gains de productivité, seuls 4% le pratiquent par crainte d'instaurer une « culture de la peur »[4].

Souvent, les entreprises soupçonnées d'appliquer ces méthodes nient ou annoncent qu'elles vont les supprimer. Parfois, elles prétendent qu'il ne s'agit que d'une

1 MOUSLI.
2 HÄSSIG.
3 BERGER/HARBRING/SLIWKA, p. 3.
4 UNITE THE UNION, Papier de position.

« recommandation aux évaluateurs »[5] et parlent alors de « recommanded ranking » (Unilever[6], HSBC), même si lesdits évaluateurs n'ont pas d'autre choix que de suivre la recommandation, de peur de se voir mal noter à leur tour. Dans ce cas, le résultat attendu de l'évaluation est bel et bien contraignant, malgré la présence du terme « recommandation ».

Certaines recherches ont montré que cette méthode d'évaluation couplée à la menace systématique de licencier le 10% des employés les moins bien classés, pouvait avoir des effets positifs sur la productivité, mais que ces effets étaient à court terme, et surtout marginaux[7]. D'autres études[8] ont par la suite montré que les effets négatifs l'emportaient, notamment au niveau des coûts de recrutement, de perte de savoir-faire, de motivation et de volonté des employés de contribuer à l'amélioration des profits, mais aussi des problèmes causés par l'obligation de mal noter un collaborateur dont la qualité du travail est pourtant bonne, tels que les conflits, la démotivation, la perte de loyauté et les problèmes de santé, ainsi que les procédures juridiques qui en découlent. Certaines entreprises comme Ford, Goodyear ou Capital One ont abandonné le « forced ranking » en raison des discriminations dues à l'âge qu'il impliquait[9]. D'autres (Microsoft), ont dû affronter des actions en justice pour cause de discrimination raciale ou de genre[10].

En France, le « forced ranking » a tout d'abord été considéré comme légal, seule une application discriminatoire ou visant à contourner la procédure en cas de licenciement économique ne l'étant pas. En 2011, la Cour d'appel, dans un arrêt du 8 septembre, a commencé par ne considérer licites que les quotas « indicatifs » et s'appuyant sur des « critères objectifs de compétences ». Plus récemment, la Chambre sociale de la Cour de Cassation a, dans un arrêt du 27 mars 2013, posé le principe que « la mise en œuvre d'un mode d'évaluation reposant sur la création de groupes affectés de quotas préétablis que les évaluateurs sont tenus de respecter est illicite ». Un arrêt de la Cour d'appel de Toulouse du 21 septembre 2011 avait déjà relevé qu'un tel système serait illicite quand bien même la mise en œuvre des évaluations individuelles serait totalement régulière.

---

5 BECKMANN (Université de Bâle), cité par OBERHUBER/BREITINGER.

6 GRAVEN.

7 ASSAD. BERGER/HARBRING/SLIWKA, pp. 30 s., constatent p. ex. une augmentation à court terme de la productivité de 8%, suivie de fortes chutes en raison de la diminution de la motivation des travailleurs qui n'obtiennent pas les notes, et donc les bonus, escomptés. SCULLEN (Université Drake à Des Moines ; cité par Business Week, No. 3966, 2006, p. 26) constate une hausse de la productivité de 16% les deux premières années, hausse qui passe à env. 6% les deux années suivantes avant de retomber à zéro une dizaine d'années après l'introduction du forced ranking.

8 DONALDSON, Performance Management : Forced Ranking et DEVELOPMENT DIMENSIONS INTERNATIONAL, cités par ASSAD ; GARCIA/TOR, pp. 107 s. ; LAWLER ; VAISHNAV ET AL.

9 OSBORNE/MCCANN.

10 OLSON ; OSBORNE/MCCANN et les références citées.

De nombreux syndicats se sont élevés contre ces méthodes, en Suisse et à l'étranger. Dans notre pays, il y a eu notamment des interventions de l'Association suisse des employés de banque (ASEB), du syndicat du personnel des transports SEV ou de syndicats de la fonction publique comme l'Association du Personnel de la Confédération (APC). En revanche, leur licéité n'a à notre connaissance jamais été portée devant les tribunaux.

II. Problèmes posés par le « forced ranking »

La majorité des études qui se sont penchées sur les conséquences des évaluations forcées s'accordent sur le fait qu'elles encouragent la concurrence à outrance, le découragement, le sentiment d'infériorité voire d'inutilité, le favoritisme, la pression, voire le mobbing[11], tant entre collègues de travail de même niveau hiérarchique que dans les relations verticales, à plus forte raison si l'évaluateur est lui-même évalué et que sa note dépend des quotas de l'évaluation forcée de ses subordonnés. Cette méthode peut aussi mener les cadres à perdre un temps considérable à négocier des faveurs avec leurs pairs dans le but d'améliorer leur propre évaluation ou de se répartir les mauvaises notes devant être attribuées pour que les quotas soient respectés. Elle peut aussi pousser les cadres à renoncer, par facilité, à évaluer leurs subordonnés avec des méthodes plus pertinentes, mais moins faciles à mettre en œuvre. En outre, elle peut pousser les collaborateurs à fuir le contact et la collaboration des bien notés, de peur d'être mal noté par comparaison[12]. Chez Amazon, elle incite aussi les responsables d'équipe à incriminer, comme dans le cadre d'un procès, les membres performants des autres équipes, dans le but d'éviter que de bons éléments de sa propre équipe ne soient licenciés, ce qui tirerait son évaluation vers le bas[13].

Les évaluations forcées ont pour effet d'être discriminantes dans leurs conséquences. En effet, selon une enquête menée par le Prof. Franz SCHULTHEISS (université de Saint-Gall) dans une grande banque suisse, les facteurs suivants ont tendance à influencer négativement le classement des salariés concernés lors du « forced ranking » : le sexe (le fait d'être une femme), l'âge (>55 ans), le fait d'avoir des enfants (notamment en âge scolaire), les handicaps, le niveau de formation, le fait de travailler à temps partiel (ce qui touche à nouveau plus particulièrement les femmes). Ces résultats corroborent ceux d'autres études[14]. En outre, certains autres facteurs influencent négativement le classement, comme le lieu de domicile ou, dans une entreprise issue d'une fusion, le fait

11 RIGOTTI (Université de Mainz)/BECKMANN (Université de Bâle), cités par OBERHUBER/BREITINGER, N 5.

12 HILL.

13 KANTOR/STREITFELD.

14 BORNEMANN, cité par OBERHUBER/BREITINGER N 5.

d'être issu du plus petit des partenaires de la fusion. Donc, outre le fait qu'ils ne sont pas uniquement évalués sur leurs propres prestations de travail, les salariés peuvent voire leur évaluation se dégrader encore plus pour d'autres raisons.

Comme il est presque impossible d'évaluer de manière objective, les salariés seront en outre rarement d'accord avec une évaluation négative, d'autant plus si celle-ci repose sur un résultat prédéterminé. Enfin, ces évaluations auront des effets à long terme, car elles peuvent influencer durablement la carrière et la progression professionnelle des personnes concernées, qui pourront se voir refuser des promotions, ou les formations qui peuvent y mener, en raison d'une mauvaise note à l'évaluation.

Les évaluations forcées sapent par ailleurs le climat de travail des équipes. En effet, encourager la concurrence entre collègues collaborant étroitement à un ou plusieurs projets communs et en classer certains, d'autorité, comme étant insuffisants nuit à la bonne collaboration et à la motivation[15]. Cela peut aussi pousser certains collaborateurs, même bien notés, à saboter sciemment le travail de leurs collègues[16]. Cette tendance peut s'aggraver encore si c'est l'équipe qui évalue elle-même ses membres. Scott SEDAM résume ainsi les effets du « forced ranking » : « Si vous évaluez les dix membres d'une équipe selon le schéma « deux bons, sept moyens et un mauvais, vous obtiendrez » : Une superstar qui ne va pas tarder à quitter le groupe parce qu'elle aura été promue, une star suspecte qui finira par devenir improductive à force de tout faire dans l'unique but de conserver son statut, trois frustrés qui pensent qu'on aurait dû les choisir parmi les « bons » et qui se demandant ce qu'ils ont fait faux, trois paranoïaques morts de peur à l'idée d'être les prochains qui seront classés « mauvais » et le dernier qui travaille sans pression et sans motivation parce qu'il sait qu'il sera le prochain à être viré. En d'autres termes, vous avez juste détruit une équipe. » [17]

Enfin, les évaluations (même si elles ne se font pas sous la forme d'un « forced ranking ») posent problème en raison de la numérisation de l'économie. En effet, dans une économie numérique, la rémunération (des entreprises comme des travailleurs) est plus basée sur la performance relative des divers acteurs (celui qui propose la meilleure offre emporte la totalité du marché) que sur leur performance absolue (rémunération en fonction des biens produits)[18]. Cela est encore accentué lorsque l'organisation du travail tout entière est définie par des algorithmes tenant notamment compte des évaluations[19]. Celui qui reçoit une évaluation moins bonne que ses collègues (quelle qu'en soit la raison), subit donc des désavantages beaucoup plus importants.

---

15 OSBORNE/MCCANN et les références citées.

16 SUTTON (Université de Stanford), cité par MOUSLI (cf. note 1).

17 SEDAM.

18 DEGRYSE, pp. 45 s.

19 Voir l'exemple d'Amazon cité par DEGRYSE, p. 43.

Enfin, ces systèmes d'évaluation ne sont jugés ni justes ni équitables par de nombreux travailleurs qui connaissent leurs défauts. Leur emploi n'est donc pas propice à assurer la bonne réputation de l'employeur.

III. Considérations juridiques

A. Droit de l'employeur d'évaluer

L'employeur a le droit d'évaluer son personnel et la façon dont il accomplit ses tâches contractuelles. Cela fait partie de son droit de donner des directives (et de vérifier qu'elles ont bien été exécutées). Cela fait également partie de son devoir de protéger la personnalité de son personnel (art. 328ss. CO), en veillant à ce qu'on lui confie des tâches pour lesquelles il est qualifié, le cas échéant qu'on lui propose les formations continues qui lui permettent de rester à la page ou de développer les nouvelles compétences qu'exigent d'éventuelles nouvelles tâches. L'évaluation est donc en principe justifiée par un intérêt prépondérant de l'employeur, voire du travailleur.

Toutefois, et c'est important, la prestation de travail ne contient pas d'obligation de résultat, mais seulement de moyen[20]. L'évaluation ne pourra donc pas porter exclusivement sur le résultat de la prestation de travail, qui ne peut être qu'un indicateur parmi d'autres pour évaluer le travail, mais devra aussi porter sur la façon dont la prestation est effectuée, quel qu'en soit le résultat. Il faut aussi ajouter que, dans bien des cas, il est très difficile, voire totalement impossible de quantifier le résultat d'une prestation de travail. Ce sera notamment le cas lorsque cette prestation correspond non pas à la production d'un certain nombre de biens ou au règlement d'un certain nombre de dossiers, mais à une attitude à adopter face à des usagers, des clients ou des collègues[21].

En évaluant, l'employeur doit cependant toujours protéger la personnalité de son personnel (art. 328 CO). Il ne peut donc pas avoir recours à des méthodes qui la violent ou qui en encouragent la violation. Une évaluation qui porte sur le « savoir-être » des salariés et qui conclut à ce qu'un travailleur doit « modifier sa personnalité » ou, dans le cas du « forced ranking », le pousse à s'adapter pour recevoir une bonne note n'est par exemple certainement pas compatible avec l'obligation de protéger la personnalité[22]. L'employeur ne peut pas non plus évaluer son personnel en fonction de critères étrangers à l'accomplissement du contrat de travail. Il ne peut enfin pas restreindre les critères d'évaluation de telle sorte que les critères retenus donnent une image incomplète, voire

[20] Cf. p. ex. DUNAND, N 10 *ad* art. 319 CO ; WYLER/HEINZER, p. 20 ; STAEHELIN, N 8 *ad* art. 319 CO.
[21] WAEBER, p. 22.
[22] WAEBER, p. 24.

erronée, de la prestation de travail. Ce sera par exemple le cas lorsque l'évaluation ne porte par exemple que sur le nombre de dossiers traités, indépendamment de la qualité du travail fournie. Pareille évaluation purement quantitative est encore moins admissible si elle a pour effet de diminuer la qualité des prestations, par exemple si les travailleurs sont incités à bâcler leur travail pour « faire du chiffre ». A contrario, une évaluation purement qualitative fondée sur des critères subjectifs, confus, voire manipulables en fonction des intentions ou de l'humeur de l'évaluateur, peut aussi porter atteinte à la personnalité des travailleurs. Ce sera par exemple le cas d'une évaluation fondée sur une notion aussi floue que le « savoir-être »[23].

Enfin, en cas de difficultés conjoncturelles, les objectifs doivent être adaptés au climat des affaires ; exiger que l'on atteigne des objectifs devenus impossibles à atteindre en raison d'une dégradation de la conjoncture ou de la situation économique de l'entreprise n'est pas conforme à l'obligation de protéger la personnalité.

B. Droit des salariés face à l'évaluation

Si les salariés ont le droit de ne pas se voir attribuer des tâches qu'ils ne sont pas en mesure d'accomplir et donc à ce que leur employeur évalue régulièrement si leurs compétences sont à jour ou si des mesures de soutien telles que formation continue sont nécessaires, le droit à la protection de la personnalité ne leur confère pas de droit à une évaluation régulière[24]. Le droit à un certificat de travail intermédiaire (art. 330a CO) ne donne pas non plus droit à une telle évaluation[25]. De plus en plus de travailleurs demandent régulièrement l'établissement de tels certificats intermédiaires, en particulier ceux d'un âge avancé ou ceux qui travaillent dans des entreprises pouvant être potentiellement restructurées. Pour ces travailleurs, il est important de pouvoir démontrer que leur prestation de travail donne toujours satisfaction à l'employeur. L'établissement d'une certification intermédiaire ne nécessite cependant pas une évaluation complète et précise du travailleur et de ses prestations. Souvent ces certificats se contentent de rappeler laconiquement que le travail donne satisfaction.

La doctrine est peu disserte sur les conditions qui rendent l'évaluation licite. Selon FISCHER, à l'avis duquel nous nous rallions, les travailleurs ont droit à une évaluation complète, conforme à la vérité, concrète et individuelle. En outre, l'employeur doit faire preuve de bienveillance lorsqu'il évalue[26].

---

23 JEAN-PIERRE LE GOFF, cité par WAEBER N 21, p. 23.

24 STREIFF/VON KAENEL/RUDOLPH, N 2a *ad* art. 330a CO. Opinion contraire : FISCHER, N 9.

25 FISCHER, N 9.

26 FISCHER, N 10.

Les travailleurs doivent en outre être informés à l'avance des critères d'évaluation, lesquels doivent être objectifs et transparents, afin qu'ils sachent ce qu'ils doivent faire pour s'y conformer. L'évaluation est en effet une conséquence du droit de donner des directives. L'employeur ne peut donner des directives que si ses salariés peuvent les accomplir. L'évaluation ne peut donc pas porter sur des critères essentiellement subjectifs ou vagues comme « l'esprit d'entreprise », à moins que ces critères n'aient auparavant été explicités de manière à ce que chacun sache ce qu'il doit faire pour s'y conformer.

Les travailleurs ont également le droit d'être évalué par quelqu'un qui est compétent en matière d'évaluation, qui a donc été formé pour cela, qui maîtrise le domaine de compétences de l'évalué (cf. *infra* F) et qui est en mesure d'évaluer sans contraintes. L'évaluation « par les pairs » est donc à éviter si les pairs n'ont pas été formés pour évaluer, à plus forte raison si leur façon d'évaluer leurs collègues à un impact sur leur propre évaluation, ou sur leurs propres conditions de travail et de carrière.

Les salariés ont aussi le droit de ne pas être évalués de manière arbitraire. Si l'évaluation à une quelconque conséquence sur les conditions de travail (p. ex. augmentation salariale) ou de carrière (p. ex. promotion), elle doit se faire selon des critères précis, transparents et connus. Et l'évaluation doit être conforme à la réalité : qui est jugé « bon » en fonction des critères doit être classé comme tel et pas rétrogradé pour la seule raison qu'il y a trop de « bons ». Selon la prof. Antoinette WEIBEL (Université de St. Gall), une évaluation fondée sur une courbe de Gauss est fondée une « erreur statistique », car elle compare des critères qui n'ont aucun lien entre eux et sont choisis de manière arbitraire[27]. A n'en pas douter le « forced ranking » ne remplit pas ce critère de conformité à la réalité (cf. aussi *infra* C).

Les salariés ont enfin le droit d'être évalués pour eux-mêmes, pour autant que cela soit possible. Lorsqu'ils sont évalués, c'est leurs prestations et leurs compétences qui doivent jouer un rôle, pas une contrainte extérieure. Si c'est une équipe tout entière qui est évaluée, seuls le comportement et les prestations de l'équipe en tant que telle doivent jouer un rôle. Et chaque membre a le droit d'être aussi évalué pour lui-même, de manière séparée, pour autant que l'on puisse réellement individualiser ses prestations. Cela dit, l'évaluation individuelle au sein d'une équipe est souvent très mal vue par les travailleurs, et peut avoir pour effet de générer de la concurrence entre les membres d'une même équipe, voire des règlements de compte[28].

[27] HR Today du 09 décembre 2014. Les problèmes de validité statistique du modèle ont également été discutés par CHATTOPADHAYAY/GHOSH et MEISLER.

[28] WAEBER, p. 24.

C. Respect de la protection des données

Les évaluations sont des données personnelles et tombent donc sous le coup de la LPD. L'employeur est autorisé à récolter ces données, pour autant qu'elles portent sur les aptitudes du travailleur à remplir son emploi ou sont nécessaires à l'exécution du contrat de travail (art. 328b CO). Les réflexions ci-dessus s'appliquent lorsqu'il s'agit de déterminer si l'évaluation remplit bel et bien ces critères de licéité.

Une évaluation forcée ne remplit à notre sens pas ces critères, pour les raisons suivantes. Elle ne porte en premier lieu pas sur les aptitudes du travailleur à remplir son emploi, mais se base plutôt sur le quota imposé étant donné que le résultat (lequel porte éventuellement sur ces aptitudes) peut être modifié en fonction du quota. Elle ne respecte par ailleurs pas le principe de la proportionnalité et de la bonne foi (art. 4 al. 2 LPD), étant donné que le classement dans telle ou telle catégorie peut dépendre au final non pas de ce qui a été évalué, mais du quota imposé. La simple possibilité que le résultat soit corrigé pour respecter le quota est à notre avis contraire aux règles de la bonne foi. La possibilité que le résultat soit corrigé contrevient enfin au principe de la qualité des données (art. 5 al. 1 LPD). En effet, si un classement dans une catégorie ou une autre est modifié a posteriori, non pas à cause des aptitudes du travailleur, mais à cause du quota, l'exactitude des données n'est pas respectée, car le classement ne correspond au final pas à la réalité. Les salariés concernés par une évaluation forcée peuvent, à ce titre, exiger la correction des données inexactes, en particulier la correction de l'évaluation afin d'être classés dans la bonne catégorie (art. 5 et 15 al. 1 LPD). C'est à l'employeur qu'incombe le fardeau de la preuve de l'exactitude des données[29].

D. Discrimination de genre

Plusieurs enquêtes concernant le « forced ranking » ont montré que les femmes ont plus de chances d'y être moins bien classées que les hommes. C'est aussi le cas des personnes travaillant à temps partiel, majoritairement des femmes (cf. *supra* II). Si le résultat des évaluations forcées aboutit à des différences systématiques entre femmes et hommes, il s'agit d'une discrimination indirecte prohibée par l'art. 3 LEg ; le système d'évaluation est en soi neutre du point de vue du genre, mais son résultat reflète une discrimination. L'employeur ne pourra guère justifier ces pratiques par des différences objectives des prestations de travail évaluées. En effet, pour respecter les quotas, l'employeur aura souvent dû classer des salariés dans une autre catégorie que celle où il les aurait classés en l'absence de quotas imposés. Les raisons de cette évaluation différente ne sont pas à

[29] STREIFF/VON KAENEL/RUDOLPH, N 16 *ad* art. 328b CO.

chercher dans une différence des prestations fournies, mais bien dans l'obligation de remplir, a posteriori, le quota imposé.

E. Risque de mobbing

D'autres enquêtes sur les évaluations forcées montrent que ces pratiques ont tendance à encourager le mobbing (cf. *supra* II.). Or, de par son obligation de protéger la personnalité de ses salariés (art. 328), l'employeur est tenu de tout mettre en œuvre pour éviter le mobbing, en particulier la mise à l'écart de salariés par leur hiérarchie ou leurs collègues. Il doit donc renoncer à tout système d'évaluation propre à favoriser ces dérives.

Dans un arrêt récent consacré au mobbing, le Tribunal fédéral a par ailleurs rappelé que l'art. 6 LTr prévoit que, dans le but de prévenir les atteintes à la santé des travailleurs, l'employeur est tenu de prendre toutes les mesures dont l'expérience a démontré la nécessité, que l'état de la technique permet d'appliquer et qui sont adaptées aux conditions d'exploitation de l'entreprise[30]. A contrario, l'employeur doit renoncer aux méthodes dont l'expérience a démontré qu'elles étaient propices à générer des atteintes à la santé. Comme il est avéré que l'emploi du « forced ranking » induit un risque important de mobbing, l'employeur doit donc y renoncer. Par ailleurs, l'emploi d'une telle méthode doit être considéré comme un risque psycho-social. Enfin, face à un cas concret de mobbing, l'usage de « forced ranking » devra être considéré comme circonstance aggravante lorsqu'il s'agira de déterminer la responsabilité de l'employeur.

F. L'évaluateur

La personne de l'évaluateur joue un rôle déterminant dans la licéité d'une évaluation. Afin que l'évaluation puisse être considérée comme équitable, il faut que l'évaluateur soit lui-même en mesure d'apprécier les qualités des évalués de manière objective et hors de toute contrainte extérieure. En premier lieu, l'évaluateur doit connaître personnellement l'évalué pour être en mesure d'évaluer son travail. Cette condition peut paraître trop évidente pour qu'on la mentionne, mais il arrive fréquemment que, dans des entreprises multinationales ou actives sur plusieurs sites géographiquement très éloignés, les membres des équipes qui collaborent au même projet ne se rencontrent jamais. Ensuite, celui qui évalue doit être doté de compétences suffisantes pour juger de la qualité de la prestation de travail. Il n'est par exemple pas admissible qu'un économiste ou un juriste dirigeant un service de recherche pédagogique évalue la qualité scientifique du travail des chercheurs placé sous ses ordres.[31] L'évaluateur ne saurait en outre se trouver en situation de concurrence avec

[30] TF 2C_462/2011 du 09 mai 2012, c. 4.1.
[31] WAEBER, p. 23.

l'évalué, car cela risquerait d'altérer son jugement et de le pousser à donner des évaluations plus négatives que nécessaire. Si l'évaluation par les pairs est en principe admissible, il ne faut pas qu'une mauvaise évaluation par ses collègues ait des conséquences sur sa propre carrière. Le même raisonnement vaut lorsque l'évaluation de l'évaluateur lui-même dépend des notes qu'il va distribuer : si sa propre note dépend du respect de quotas, on ne saurait considérer comme équitables les évaluations qu'il fait de ses subordonnés.

G. L'évaluation par un évaluateur externe

1. L'évaluation par les clients et les usagers

Avec la numérisation de l'économie est apparue une tendance à évaluer systématiquement les prestations des entreprises et les collaborateurs qui les fournissent. Ces évaluations ne sont pas le fait de cadres ou de collègues, formés ou non à l'évaluation, mais des seuls clients.

Ainsi, la plupart des services-clients mènent des enquêtes de satisfaction dès qu'une prestation a été fournie ou qu'il y a eu un contact entre le client et le service-client. La façon dont le ou les travailleurs ont fourni le service est systématiquement analysée. Cette tendance touche désormais tous les secteurs. On la trouve bien entendu chez les prestataires de service en ligne et gestionnaires de plateforme comme Uber, qui demande à ses clients d'évaluer ses chauffeurs après chaque course en leur accordant un certain nombre d'« étoiles ». Mais elle touche aussi les services offerts uniquement dans le Monde « réel » : p. ex. l'Aéroport de Genève met à la disposition de ses clients de nombreuses bornes où l'on peut cliquer sur l'« emoji » qui correspond à sa satisfaction vis-à-vis de toutes sortes de services : temps d'attente au contrôle de sécurité, déroulement dudit contrôle, propreté des sanitaires, achalandage des boutiques, etc. Il y a aussi l'exemple d'une banque cantonale romande, qui a récemment envoyé des questionnaires de satisfaction à des clients sélectionnés, qui portaient essentiellement sur les collaborateurs auxquels ils avaient eu à faire.

Ces évaluations n'ont en général qu'une valeur indicative et ne se rapportent pas à la prestation d'un travailleur en particulier, ou d'un groupe identifié d'entre eux. Mais elles peuvent aussi porter sur l'attitude ou les compétences d'un ou plusieurs travailleurs en particulier et avoir des conséquences sur la poursuite de leur contrat de travail, sans que le client qui évalue n'en ait forcément conscience. Ainsi, chez Uber, l'accumulation de mauvaises évaluations a pour effet de restreindre le nombre de fois où il sera fait appel aux services des chauffeurs concernés[32]. Et, chez l'entreprise de nettoyage Batmaid, si les

[32] PÄRLI, N 45.

travailleurs obtiennent régulièrement l'évaluation maximale, leur salaire sera majoré[33]. Cela est très problématique. D'une part, parce que les évaluations données par les clients ne sont que très rarement le fait de spécialistes de l'évaluation et ne remplissent que rarement les conditions posées sous *supra* F). Comme ils ne savent pas quel impact l'évaluation peut avoir sur la carrière du travailleur évalué, ils n'évalueront pas forcément avec la bienveillance nécessaire. En outre, le recours à des notes pour évaluer la qualité d'un service n'est que très rarement fiable[34]. Enfin, indépendamment de leurs compétences réelles en matière d'évaluation, l'évaluation par les clients peut être totalement tronquée par leur humeur du moment. Ainsi, celui qui fait appel à un service d'assistance technique pour un problème informatique qu'il considère comme grave (soit en raison de sa gravité réelle ou subjective, soit en raison du temps perdu à le résoudre) et qui n'a pas pu être résolu sera certainement d'une humeur qui ne le poussera pas à évaluer favorablement le travailleur qui a tenté en vain de l'aider. Enfin, le travailleur évalué n'a que rarement la possibilité de donner son point de vue sur les évaluations qu'il reçoit, ne serait-ce qu'en raison de leur nombre.

Nous en concluons donc que l'évaluation par les clients ne doit pas avoir à elle seule d'impact sur la poursuite des relations de travail, à moins bien entendu qu'on puisse garantir que l'évaluation respecte les conditions évoquées plus haut. Une mauvaise évaluation ne pourra donc être portée au dossier du travailleur que si elle respecte les principes de la bonne foi et de l'exactitude des données (cf. *supra* C.) et ce dernier devra au moins avoir la possibilité de donner son explication sur le contexte. Si l'employeur prend des mesures, par exemple un licenciement, en s'appuyant sur une critique négative ou de mauvaises évaluations récurrentes émises par un ou plusieurs clients, il devra étayer ces dernières et donner au travailleur la possibilité de s'exprimer à leur sujet. L'employeur doit aussi, en vertu de son devoir de protection (art. 328), éviter que ses travailleurs ne soient confrontés à des évaluations bâclées, sans aucun fondement, fondées sur l'humeur des clients et sur lesquelles ils n'ont pas la possibilité d'apporter leur propre son de cloche. En effet, être confronté régulièrement à des remarques négatives injustifiées, surtout si elles sont le fait de personnes qui ne connaissent pas grand-chose ni au métier du travailleur, ni à ses activités concrètes, ni à l'art d'évaluer, risque de porter atteinte à l'estime de soi des travailleurs et, partant à leur santé psychique.

2. L'évaluation secrète (clients mystères et achats tests)

Il est de plus en plus fréquent que les prestations de travail soient évaluées de manière secrète par de faux clients, engagés par l'employeur, par des associations ou par les autorités, dont la tâche est d'évaluer le personnel en se faisant passer pour un client

[33] « frc mieux choisir » n° 88, mai 2016, p. 7.

[34] BENAVENT, p. 114, 128 et les références citées.

(« clients mystères »), respectivement de contrôler le respect de certaines normes légales (« achats tests »).

a) Les clients mystères

Les clients mystères sont engagés par l'employeur pour se faire passer pour un client « normal » et évaluer la façon dont les travailleurs interagissent avec lui, lui fournissent la prestation souhaitée et répondent à ses attentes. Certains doivent se faire passer pour des clients habituels, d'autres ont pour mission de jouer les clients inhabituellement exigeants, pointilleux, voire quérulents. Certains iront jusqu'à se montrer particulièrement pénibles, quitte à pousser le personnel à l'erreur.

Du point de vue de l'employeur, il est intéressant de pouvoir évaluer son personnel « en conditions réelles ». En effet, lorsque c'est l'employeur qui « fait un tour » dans l'entreprise, il va de soi que les travailleurs appliqués feront preuve d'un zèle appuyé, afin d'être bien considérés par leur patron. L'évaluation pourrait donc être biaisée. En revanche, s'ils sont évalués lorsqu'ils servent un client qu'ils croient standard, ils agiront comme d'habitude et le résultat de l'évaluation sera plus pertinent.

Toutefois, les clients mystère ne constituent à notre sens un moyen licite d'évaluation qu'à des conditions restrictives. Il faut d'abord que les clients mystères remplissent les critères posés sous *supra* F) à propos de la personne qui évalue. Ensuite, il faut que le personnel soit informé de leur passage potentiel, afin qu'il sache qu'il peut être évalué non pas par un évaluateur interne ou un supérieur hiérarchique, mais par n'importe quel client. Les critères d'évaluation doivent aussi être connus, ainsi que chaque travailleur sache ce qu'il faut faire pour s'y conformer. En outre, l'employeur ne devra en aucun cas tenir compte d'une évaluation menée par un client mystère ayant tout fait pour pousser le collaborateur à l'erreur. En effet, même si le personnel doit, dans certaines situations, être en mesure de réagir face à des clients très pénibles ou inhabituellement exigeants, l'obligation de protéger la personnalité (art. 328) commande à l'employeur de ne pas pousser expressément ses travailleurs à la faute. Par ailleurs, une éventuelle responsabilité du travailleur au titre de l'art. 321e serait atténuée par le fait que l'employeur, par le biais de son représentant, l'a incité à commettre une erreur. Enfin, en cas de mauvaise réaction face à un client mystère, l'employeur devra tenir compte du contexte, notamment d'autres éléments qui peuvent altérer la qualité du travail du travailleur concerné, comme une mauvaise santé, une situation familiale difficile ou des soucis de nature financière. En effet, chaque travailleur, même les plus performants, peut avoir son jour de méforme, un jour « sans ». Il serait injuste qu'il subisse les conséquences d'une mauvaise évaluation réalisée lors d'un pareil moment de faiblesse, alors que, si elle avait été effectuée un autre jour, son résultat aurait été bien meilleur.

b) Les achats tests

Les achats tests consistent à envoyer des mineurs acheter des boissons alcoolisées, afin de contrôler si les commerces respectent la législation qui leur interdit pareille transaction. Ce n'est pas un moyen de contrôle de l'employeur, mais plutôt d'une collectivité publique, bien que des associations de prévention mènent régulièrement des expériences d'achats tests afin de montrer que la législation en matière de vente d'alcool n'est pas parfaitement respectée. Des achats-tests ont aussi été effectués pour vérifier le respect de l'interdiction de vendre des cigarettes à des mineurs[35]. Ces achats tests nécessitent une base légale pour que leur résultat puisse être exploité par la Justice, car il s'agit d'une investigation secrète au sens de l'art. 286 CPP[36]. Le projet de révision totale de la loi sur l'alcool[37], qui prévoyait la création d'une telle base légale[38], ayant été définitivement classé par le Conseil des Etats le 16 décembre 2015 et par le Conseil national le 17 décembre 2015, cette base légale fait actuellement défaut au niveau fédéral. Malgré l'absence de base légale, des organisations de prévention continuent leurs campagnes d'achats tests, ce qui n'est nullement interdit, de même que de dénoncer les éventuels contrevenants à la Justice[39].

Indépendamment de l'existence d'une base légale, il convient de s'interroger sur les conséquences des achats tests sur le contrat de travail. Vendre de l'alcool à un mineur est interdit, ce qui peut justifier un licenciement, voire un congé avec effet immédiat pour juste motif (art. 337 CO). Un licenciement ne sera toutefois pas justifié, ou sera abusif (art. 336 CO), si l'employeur a incité son personnel à violer la loi, explicitement en lui donnant la directive de vendre à tout le monde ou de ne pas contrôler l'âge des clients, ou implicitement en le poussant « à faire du chiffre ». La question devra aussi se poser si l'employeur ne prend pas les mesures nécessaires pour protéger son personnel de l'insistance des clients mineurs, par exemple en indiquant clairement à la clientèle que la loi sur l'âge minimal d'achat sera respectée et que le personnel peut demander une pièce d'identité s'il y a un doute sur l'âge du client. Enfin, en cas de négligence, par exemple si le travailleur ne demande pas de pièce d'identité à un jeune dont l'apparence laisse objectivement à penser qu'il a atteint l'âge légal ou parce que, dans un festival ou une fête populaire, tous les stands de boissons environnants ne respectent visiblement pas la

35 http://www.rts.ch/info/regions/fribourg/8055931-trop-de-commerces-vendent-des-cigarettes-a-des-jeunes-a-fribourg.html (consulté le 23.12.16).

36 TF 6B_334/2011 du 10 janvier 2012 ; Message sur la Loi sur l'alcool, FF 2012 1111 (1173 ss).

37 Objet parlementaire 12.020, Message sur la loi sur l'alcool, FF 2012 1111. Le Conseil fédéral envisage toutefois de faire une nouvelle proposition, cf. FF 2016 3503.

38 Art. 13 P-LCal in FF 2012 1291 ss.

39 FF 2012 1174. La campagne la plus récente date de l'automne 2016, cf. « 24 heures du 22.9.16 » disponible en ligne sur : http://www.24heures.ch/vaud-regions/jeunes-parviennent-acheter-alcool/story/18230702 (consulté le 23.12.16).

législation ou ne demandent pas de pièce justificative de l'âge des clients, il n'y aura pas de juste motif de congé avec effet immédiat et le licenciement pourra être abusif.

IV. Conclusion : Les conditions de la licéité de l'évaluation

L'employeur a le droit d'évaluer son personnel. Parfois, il en a le devoir, ne serait-ce que vous vérifier l'adéquation de ses compétences avec les tâches qu'il lui assigne. Mais il ne peut pas faire n'importe quoi. L'évaluation doit être objective et bienveillante et les travailleurs doivent savoir ce qui sera évalué et ce qu'il faut faire pour se conformer aux attentes. Ils doivent aussi pouvoir donner leur position sur les évaluations reçues. L'évaluation doit en outre être menée par une personne qualifiée, tant au niveau des techniques d'évaluation que des compétences à évaluer.

Le « forced ranking » ne respecte à notre avis aucune des conditions qui légitiment l'évaluation du travailleur par l'employeur. C'est en effet une méthode qui ne permet pas une évaluation de la prestation de travail bienveillante, objective et conforme à la vérité. Elle aggrave le risque de violation de l'obligation de protéger la personnalité des travailleurs, voir, pis constitue en elle-même une telle violation. Les études qui se sont penchées sur ses conséquences parviennent en outre à la conclusion que, outre ses effets économiques peu convaincants, voire totalement négatifs à terme, cette méthode est propice aux discriminations et au mobbing et doit dont être bannie en raison de l'obligation de l'employeur de protéger les travailleurs. Enfin, un licenciement qui suit une évaluation ne respectant pas les critères évoqués précédemment sera un fort indice de licenciement abusif.

En ce qui concerne l'évaluation par les clients, l'employeur ne devrait pas se servir de leur résultat pour décider de la poursuite des relations de travail. En effet, il est souvent impossible de garantir que le client donne un avis véritablement objectif et ne cède pas à la tentation de « passer sa hargne » sur le travailleur auquel il a eu affaire. Bien souvent, les travailleurs n'ont pas la possibilité de donner leur point de vue s'ils reçoivent une évaluation négative. Enfin, l'évaluation par des achats tests ou des clients mystères ne doit être admise que de façon très restrictive, à plus forte raison si ce type d'évaluation est menée dans le but de pousser les travailleurs à commettre des erreurs.

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.

ASSAD VICTOR, Forced Ranking : The good, the bad, the ugly, and what to do about it, *in* : Forbes, 18 mai 2015.

BENAVENT CHRISTOPHE, Plateformes ; sites collaboratifs, marketplaces, réseaux sociaux... Comment ils influencent nos choix, Roubaix 2016.

BERGER JOHANNES/HARBRING CHRISTINE/SLIWKA DIRK, Performance Appraisals and the Impact of Forced Distribution : An Experimental Investigation, IZA Discusssion Paper N° 5020, juin 2010.

CHATTOPADHAYAY RACHANA/GHOSH ANIL KUMAR, Performance appraisal base on a forced distribution system : its drawbacks and remedies, *in* : International Journal of Productivity and Performance Management, Vol. 61/8, 2012, pp. 881 ss.

CONSEIL FÉDÉRAL, Message concernant la révision totale de la Loi sur l'alcool, FF 2012 1111 (cité : Message sur la Loi sur l'alcool).

DEGRYSE CHRISTOPHE, Les impacts sociaux de la digitalisation de l'économie, Working Paper 2016.02 de l'ETUI, Bruxelles 2016.

DUNAND JEAN-PHILIPPE, Commentaire de l'art. 319 CO, *in* : Jean-Philippe Dunand/Pascal Mahon (éds.), Commentaire du contrat de travail, Berne 2013.

FISCHER PASCAL, Die Mitarbeiterbeurteilung aus juristischer Perspektive, *in* : Jusletter 12 février 2007.

GARCIA STEPHEN M./TOR AVISHALOM, Rankings, standards, and competition : Task vs. scale comparisons, *in* : Organizational Behavior and Human Decision Processes 102/1 janvier 2007, pp. 95-108.

GRAVEN JULIA, Mitarbeiterbewertung in Deutschland « Die Schlechten ins Kröpfchen », *in* : Spiegel Karriere, 14 novembre 2013.

HÄSSIG LUKAS, UBS führt Forced Ranking durch Hintertür ein, in: Inside Paradeplatz, 15 février 2016, disponible en ligne sur : http://insideparadeplatz.ch/2016/02/15/ubs-fuehrt-forced-ranking-durch-hintertuer-ein/.

HILL ANDREW, Forced ranking is a relic of an HR tool, *in* : Financial Times, 16 juillet 2012.

LAWLER EDWARD E., Getting rid of the bottom 10%, sounds good but…, Center for Effective Organizations, Los Angeles 2002.

KANTOR JODI/STREITFELD DAVID, Inside Amazon : Wrestling Big Ideas in a Bruising Workplace, *in* : New York Times, 15 août 2015.

MEISLER ANDY, Dead Man's Curve, *in* : Workforce 82/7, juillet 2003, pp. 44 ss.

MOUSLI MARC, Le forced ranking, un système pervers, *in* : Alternatives Economiques 299, février 2011.

OBERHUBER NADINE/BREITINGER MATTHIAS, Amazon – Abschied vom Lowperformer, *in* : Zeit Online du 18 août 2015, disponible en ligne sur : http://www.zeit.de/wirtschaft/

unternehmen/2015-08/amazon-jeff-bezos-arbeitnehmer-ausbeutung-forced-ranking-mitarbeiterbeurteilung (consulté le 19.05.16).

OLSON ELIZABETH E., Microsoft, GE, and the futility of ranking employees, *in* : Fortune, 18 novembre 2013.

OSBORNE TOM/MCCANN LAURIE A., Forced Ranking and Age-Related Employment Discrimination, *in* : Human Rights Magazine, Vol. 31/2, 2004.

PÄRLI KURT, Gutachten über arbeits- und sozialversicherungsrechtliche Fragen bei Uber-Taxifahrer/innen, Bâle/Berne 2016.

SEDAM SCOTT, Rank and Yank : the curious legacy of Jack Welch, *in* : Professional Builder, 1er juin 2005.

STAEHELIN ADRIAN, Art. 319-330*a* OR. Der Arbeitsvertrag – Zürcher Kommentar, Zurich 2015.

STREIFF ULLIN/VON KAENEL ADRIAN/RUDOLPH ROGER, Arbeitsvertrag – Praxiskommentar zu Art. 319-362 OR, 7e édition, Zurich/Bâle/Genève 2012.

UNITE THE UNION, Forced Ranking in Performance Management, Papier de position, 2011, disponible en ligne sur : www.unitetheunion.org (cité : UNITE THE UNION, Papier de position).

VAISHNAV CHINTAN ET AL., Punishing by Reward : When your Performance Bell-curve Stops Working for You, International Conference of System Dynamics, Nijmegen 2006, disponible en ligne sur : http://web.mit.edu/chintanv/www/Publications/Chintan%20Vaishnav%20Punishing%20by%20Rewards%20for%20Publication%20Final.pdf (consulté le 28.04.16).

WAEBER JEAN-BERNARD, Les méthodes d'évaluation modernes et le respect des droits de la personnalité, *in* : Plaidoyer 3/10, pp. 22 ss.

WYLER REMY/HEINZER BORIS, Droit du travail, 3e édition, Berne 2014.

CAMILLE STAUFFER

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

Sommaire

		Page
I.	Introduction	344
II.	La commission paritaire et les données nécessaires au contrôle	345
	A. Les compétences de contrôle des commissions paritaires	345
	1. L'art. 357b CO et la LECCT	345
	2. La délégation des compétences à une association de contrôle	346
	3. Les compétences accordées aux commissions paritaire par la Loi sur le Service de l'Emploi	347
	4. Les compétences accordées aux commissions paritaires par les mesures d'accompagnements	348
	B. Nature des données traitées et déclaration du fichier	349
III.	La licéité de la communication de données à une commission paritaire	350
	A. Les motifs justificatifs au traitement de données par la commission paritaire	350
	1. Le consentement	350
	2. La loi	350
	3. L'intérêt public prépondérant	351
	a) L'intérêt public	351
	b) L'intérêt privé des personnes contrôlées	352
	4. Le respect des principes généraux de la LPD	354
	B. Le renseignement de l'organe paritaire selon le contrat de travail	354
	a) L'article 328b CO	355
	b) L'article 321 CO	355
IV.	Le refus de transmettre les données nécessaires au contrôle	356
	A. La sanction de la non collaboration par une peine conventionnelle	356
	B. La désignation d'un organe spécial de contrôle	357
	C. Le recours au juge civil	358
	1. La qualité pour agir d'une commission paritaire	359
	2. La requête en procédure applicable aux cas clairs	359
	a) L'admissibilité d'une demande de production de document	359
	b) La motivation de la requête	360
	3. Les autres requêtes	361
V.	Conclusion	362
Bibliographie		363

I. Introduction

La négociation et la signature de conventions collectives par les associations de travailleurs et d'employeurs d'un secteur économique laissent une grande autonomie aux partenaires sociaux. AUBERT, décrivait cette autonomie, dans un article de 1992 sur l'évolution des conventions collectives dans la perspective de l'EEE, par la phrase suivante : « Dans plusieurs domaines, en effet, l'Etat s'est abstenu de légiférer, en souhaitant que les parties aux conventions collectives adoptent elles-mêmes les règles qui leur paraissent nécessaires[1] ».

Cette liberté dans les moyens d'application d'une convention collective de travail (ci-après CCT) est, comme toute liberté, sujette à des limites. C'est celles touchant à la protection des données qui nous intéresseront ici : les traitements de données concernant travailleurs et employeurs par une commission paritaire[2] sont nombreux. Celles-ci sont parfois des données sensibles, telles que l'affiliation syndicale des travailleurs concernés, ou des informations relatives aux assurances sociales[3].

Nous avons choisi de rappeler d'abord brièvement le système de l'exécution commune, et les types de données traitées. Nous présenterons ensuite les motifs justifiant le traitement de données par la commission paritaire. Une transmission de documents doit être justifiée du point de vue de la personne qui les reçoit, mais aussi de la perspective de la personne qui les transmet. Nous examinerons donc également l'acte de renseigner une commission paritaire à la lumière du contrat de travail individuel. Pour terminer, nous passerons en revue les moyens à disposition de la commission paritaire pour obtenir des documents face à un refus de collaboration.

L'analyse de la production de documents dans les lignes ci-dessous se limite à la relation entre les employeurs et travailleurs assujettis à la CCT d'une part, et les commissions paritaires et leurs associations de contrôle d'autre part. La transmission des résultats des contrôles à une personne externe à cette relation soulève d'autres questions et enjeux, qui ne seront pas examinée ici.

---

1 AUBERT, p. 26.

2 Nous utilisons la désignation « commission paritaire » pour qualifier l'organe paritaire chargé de contrôler le respect d'une CCT. Les parties contractantes peuvent cependant faire appel à une autre désignation (cf. point II.A.1.).

3 Il est par exemple nécessaire de contrôler l'éventuel arrêt maladie d'un travailleur pour justifier un salaire versé par l'employeur inférieur de 20% au salaire minimum CCT. Le motif de l'empêchement de travail, outre la cause, n'est cependant pas nécessaire dans le cadre du contrôle.

II. La commission paritaire et les données nécessaires au contrôle

A. Les compétences de contrôle des commissions paritaires

1. L'art. 357b CO et la LECCT

Les CCT sont des « sources de droit privé avec effet normatif »[4], dont l'exécution revient aux parties contractantes. Celles-ci sont les syndicats et les associations patronales qui les ont négociées et signées. Le législateur a mis à leur disposition à cette fin l'institution de l'exécution commune, qui fait l'objet de l'art. 357b CO. BRUCHEZ décrit l'exécution commune par sa particularité à « conférer des droits directs aux parties contractantes agissant en commun – c'est-à-dire à la "communauté conventionnelle" – à l'égard des employeurs et travailleurs liés »[5].

La forme la plus souvent utilisée à ce jour est l'association[6] ou la fondation[7], qui disposent toutes les deux de la personnalité juridique. Les compétences de la commission paritaire lui sont attribuées par la CCT qui s'y rattache, et par ses statuts. La qualité pour agir en justice d'une commission paritaire sera traitée ci-après.

La Loi sur l'extension des conventions collectives de travail (ci-après : LECCT) permet de demander l'extension de la CCT à l'ensemble des employeurs et travailleurs de la branche, à des conditions précises. Contrairement à l'adhésion d'une partie contractante, ou à la signature individuelle d'une CCT[8], l'arrêté d'extension permet de rendre obligatoire le respect des clauses étendues aux entreprises et travailleurs qui ne souhaitent pas y être liés[9]. RONCORONI rappelle qu'« en englobant autant que possible tous les employeurs et

4 WYLER/HEINZER, p. 811.

5 BRUCHEZ, N 15 *ad* art. 357b CO, p. 1211.

6 Par exemple : art. 11 al. 1 CCT dans la branche des techniques du bâtiment du 1er janvier 2014 : Pour l'exécution de la CCT, il est constitué une Commission paritaire nationale (CPN) sous la forme juridique d'une association au sens des art. 60 ss du Code civil et de l'art. 357b du Code des obligations.

7 Par exemple :
Art. 22 CCRA dans l'industrie du marbre et du granit : *(al.1) Les parties conviennent de l'application commune au sens de l'art. 357b du Code des Obligations. (al. 2) Elles fondent à cet effet la « Fondation pour la retraite anticipée dans l'industrie du marbre et du granit » (MARMOR) dans le but d'appliquer et de faire appliquer la présente CCRA et elles lui confèrent tous les droits nécessaires.*

8 Art. 356b CO.

9 Art. 1 LECCT.

travailleurs d'une branche, la décision d'extension ne sert donc pas que des intérêts particuliers, mais répond également à un intérêt public[10]».

2. La délégation des compétences à une association de contrôle

Les commissions paritaires sont généralement autorisées à déléguer la détection d'infractions ou le contrôle administratif des livres de salaires à des associations de contrôle dans le cadre des tâches qui leur sont attribuées par les CCT[11].

Du point de vue de la LPD, les associations de contrôle agissent en qualité de tiers selon l'art. 10a LPD : le traitement de données personnelles peut leur être confié pour autant qu'une convention ou la loi le prévoie et que les conditions suivantes soient remplies : (lit. a) seuls les traitements que le mandant serait en droit d'effectuer lui-même sont effectués et (lit. b) aucune obligation légale ou contractuelle de garder le secret ne l'interdit.

Le traitement délégué à un tiers ne constitue pas une communication de données au sens du droit de la protection des données, puisque la personne qui délègue garde la maîtrise de celles-ci[12]. MEIER précise qu'«[i]l n'y a pas de traitement de données délégué à un tiers lorsqu'il est assuré par une succursale, un autre service ou un collaborateur au sein de la même personne morale »[13].

Si la délégation est prévue par la CCT, et donc par une convention supposant le consentement des entreprises signataires, la condition de l'absence d'une obligation de garder le secret mérite d'être examinée dans le cas de CCT étendues selon la LECCT : la directive du SECO sur la perception des contributions professionnelles prévoit une obligation de garder le secret pour les commissions paritaires[14]. L'Office fédéral a cependant élaboré un rapport dans le cadre du groupe de travail « Besoin d'amélioration de l'exécution et de la lutte contre les abus dans le cadre des mesures d'accompagnement », comportant un point sur l'organisation des missions de contrôles et les exigences minimales contractuelles que doit respecter le mandat de contrôle qui leur est fixé par les commissions[15].

---

10 RONCORONI, N 3 *ad* art. 1 LECCT, p. 392.

11 Art. 22 al. 3 CCRA dans l'industrie suisse du marbre : [la] fondation peut céder à des tiers les activités de contrôle et d'encaissement […].
Art. 25 CCT pour les échafaudeurs suisses 2012 : [la commission paritaire] *peut confier ces contrôles et enquêtes à des tiers* [...].

12 BAERISWYL, N 6 *ad* art. 10a LPD, p. 136, et les références citées.

13 MEIER, N 1201, pp. 423.

14 SECO, Directive sur les contributions professionnelles, Point 3, p. 7.

15 Rapport du groupe de travail FlaM, pp. 10, 12, 18, 28 et 29.

Bien qu'orienté vers l'application des mesures d'accompagnement, notamment le contrôle des travailleurs détachés en Suisse dans le cadre d'une prestation de service, le groupe de travail susmentionné reconnaît le rôle des commissions paritaires dans le cadre du contrôle des entreprises suisses et de surveillance du marché du travail[16]. L'obligation de garder le secret imposée aux commissions paritaires par la directive du SECO[17], déjà critiquée par HÄBERLI, qui la juge trop stricte[18] ne restreint donc pas le recours à des associations de contrôle.

Les personnes habilitées à réceptionner des données en vue d'un contrôle des conditions de travail et de salaire seront donc : les membres de la commission paritaire, les employés de la commission paritaire, ainsi que les membres et employés de l'association de contrôle.

Les personnes qui transmettent ces données sont les travailleurs et employeurs soumis à la convention, qui répondent à la sollicitation de la commission paritaire ou l'association de contrôle. La sollicitation de données peut se faire par correspondance, ou lors d'enquêtes sur le lieu de travail ou au siège de l'entreprise.

3. Les compétences accordées aux commissions paritaires par la Loi sur le Service de l'Emploi

Les commissions paritaires rattachées à une convention collective étendue selon la LECCT disposent d'une compétence de contrôle reposant sur l'art. 20 de la Loi sur la Location de service (LSE), dont l'alinéa 2 prescrit notamment que l'organe paritaire de contrôle prévu par la convention collective de travail étendue est habilité à contrôler le bailleur de services. L'art. 48d de l'Ordonnance sur le service de l'emploi (OSE) impose une obligation d'égalité de traitement entre les bailleurs de services contrôlés et les autres employeurs de la branche[19]. Le bailleur de service peut déposer une demande de désignation d'un organe de contrôle indépendant par l'application par analogie de l'art. 6 LECCT[20] (voir *infra*).

Les relations entre l'entreprise employeur de fait et le travailleur loué sont qualifiées de « quasi-contractuelles »[21], alors que celles entre l'employeur de droit et le travailleur loué d'une part et celles entre l'employeur de droit louant les services et l'employeur de fait d'autre part, sont de nature contractuelle. L'entreprise doit donc respecter son devoir d'assistance (« Fürsorgepflicht ») et son devoir de surveillance (« Überwachungspflicht »)

16 Rapport du groupe de travail FlaM, p. 4.
17 SECO, Directive sur les contributions professionnelles, point 3.5, p. 7.
18 HÄBERLI, N 45 *ad* art. 357b CO, p. 284.
19 Art. 48d al. 2 OSE.
20 Art. 48 al. 4 OSE.
21 TF 4C.155/2006 du 23 octobre 2006, c. 7.3.1.

envers le travailleur loué, en contrepartie de son droit à donner des instructions (« Weisungsrecht »)[22]. Ces obligations, à l'exception du droit à donner des instructions, reviennent aussi à l'employeur de droit. On considère aussi que « [l]e devoir de diligence et de fidélité (art. 321a CO) doit également être observé, par le travailleur temporaire, à l'égard de l'entreprise de mission (locataire de services), qui agit comme employeur de fait »[23], mais aussi envers son employeur de droit.

Les éléments justifiant le renseignement à une commission paritaire du point de vue du contrat de location de service seront donc, à notre avis, les mêmes dans le cas du contrat de location de service que dans le contrat individuel classique.

4. Les compétences accordées aux commissions paritaires par les mesures d'accompagnements

Les commissions paritaires sont également des acteurs des mesures d'accompagnement à la libre circulation des personnes, dont le but est de contrer le risque de sous-enchère sociale et salariale[24] que représente la libre circulation des personnes. L'article 7 lit. a de la Loi sur les travailleurs détachés (ci-après : LDét) prévoit que le contrôle du respect des conditions fixées dans la présente loi incombe aux organes paritaires chargés de l'application de la convention pour les dispositions prévues par une convention collective de travail étendue.

Il peut être précisé que la production des documents nécessaires au contrôle est une obligation légale pour les entreprises étrangères directement ancrée à l'art. 7 al. 2 LDét. Sa violation peut faire l'objet d'une sanction de droit pénal administratif selon l'art. 12 al. 1 lit. a LDét. Les commissions paritaires n'ont par ailleurs pas qualité pour agir si elles constatent un refus de collaborer, mais doivent transmettre le dossier à l'autorité compétente de leur canton, qui prendra les mesures nécessaires. Le SECO prescrit en effet qu'en cas de non-respect de l'obligation de renseigner de l'entreprise, « la CP (ou l'organe de contrôle) annonce systématiquement l'entreprise au canton pour que celui-ci puisse lancer une procédure de sanction[25] ».

En raison du statut particulier des entreprises étrangères et de l'exécution de prestations de service sur territoire suisse dans le cadre de l'Accord sur la libre circulation des personnes, ce point ne sera pas traité plus avant.

---

22 KULL, N 12 *ad* art. 12 LSE, p. 57, commentaire de l'arrêt du Tribunal fédéral des assurances du 30 mai 1988, *in* : JAR 1989 259.

23 MATILE/ZILLA/STREIT, p. 86, commentaire de l'arrêt du Tribunal de cassation du canton de Lucerne du 26 juin 2007, édité *in* : JAR 2008 435.

24 BRUCHEZ, Droit collectif, N 111 *ad* art. 356 CO, p. 190.

25 SECO, Directive Procédure modèle, p. 7.

B. Nature des données traitées et déclaration du fichier

Les données communiquées par les employeurs et travailleurs entrant dans le champ d'application de la CCT portent sur les conditions de travail et de salaires pratiquées dans l'entreprise. Ces données sont fournies notamment par les documents suivants : les fiches de salaires des travailleurs, leurs contrats de travail, les relevés d'heures, les coordonnées des entreprises et travailleurs contrôlés, le lieu de travail, et l'affiliation syndicale des travailleurs. Dans le rapport pour l'année 1998/1999 du Préposé fédéral à la protection des données, les documents que doivent présenter les personnes contrôlées dans le cadre d'une CCT incluent non seulement la liste du personnel et les fiches de salaires, mais également les documents liés à la comptabilité[26]. Une décision du Tribunal Arbitral du secteur principal de la construction du canton de Schaffhouse prescrit la remise à la Commission paritaire, en plus des documents déjà mentionnés, des décomptes salaires déclarés à la SUVA et à l'AVS, les décomptes liés à la LPP et l'entier de la comptabilité liée au travailleur[27].

Les fiches de salaire mentionnent souvent le numéro AVS des travailleurs faisant l'objet du contrôle, et cas échéant, les périodes de maladie, d'accident ou de maternité ayant causé une incapacité de travail. L'affiliation syndicale des travailleurs est par définition un élément connu par les commissions paritaires car elle est à la base du champ d'application personnelle d'une convention collective de travail. Il s'agit de données sensibles au sens de l'art. 3 lit. c et d LPD, dont le traitement donne lieu à des prescriptions légales particulières, notamment la déclaration du fichier.

Comme exposé ci-dessus, une commission paritaire traite des données sensibles. Elle est donc soumise, a priori, à l'obligation de déclarer le fichier de données prévue par l'art. 11a al. 3 LDP envers les personnes privées traitant régulièrement des données sensibles ou des profils de la personnalité (lit. a), ou communiquant régulièrement des données à des tiers (lit. b). La LPD prévoit cependant des exceptions à la déclaration de fichier : le maître du fichier n'est notamment pas tenu de le déclarer, selon l'art. 11a al. 5 lit. a LPD, lorsque les données sont traitées par une personne privée en vertu d'une obligation légale.

L'obligation légale d'exécution de la CCT à l'encontre des signataires et celle de traiter de la même manière les entreprises auxquelles la CCT est étendue justifient, à notre avis, la dérogation à l'obligation de déclarer les fichiers de données traitées au sens de l'art. 11a al. 5 lit. a LPD. Ces obligations sont détaillées ci-après (point III.2).

---

26 PFPDT, Rapport 1998/1999, p. 66.

27 Décision du Lokales Schiedsgericht für das Bauhauptgewerbe du canton de Schaffhouse du 23 août 1999, c. 3, *in* : JAR 2000 367.

III. La licéité de la communication de données à une commission paritaire

L'art. 12 al. 1 LPD prescrit que quiconque traite des données personnelles ne doit pas porter une atteinte illicite à la personnalité des personnes concernées. L'article suivant de la loi prévoit les motifs justificatifs levant l'illicéité : il s'agit notamment du consentement de la victime, d'un intérêt prépondérant privé ou public, ou de par la loi. Nous présenterons d'abord le consentement, puis la loi, et enfin l'intérêt public prépondérant se rapportant à l'action des commissions paritaires pour l'application de CCT. Le rôle des principes de la protection des données sera ensuite rappelé.

A. Les motifs justificatifs au traitement de données par la commission paritaire

1. Le consentement

La première situation qui justifie le traitement des données par les commissions paritaires est le consentement des personnes contrôlées. Une majorité des travailleurs et employeurs soumis à la CCT reconnaissent la compétence de la commission paritaire pour en vérifier l'application et acceptent de transmettre les documents listés ci-dessus.

Le fait d'adhérer à une association signataire ou de signer individuellement une CCT correspond à un consentement aux contrôles d'application prévu par son texte. Le motif justificatif de l'art. 13 al. 2 lit. a. LPD, soit un intérêt privé prépondérant de la commission paritaire existe donc envers pour les entreprises signataires. Rien n'empêche cependant, en pratique, une entreprise signataire de refuser expressément un contrôle. La commission paritaire devra alors justifier sa demande par les autres motifs ou recourir au moyen IV.

2. La loi

Les parties contractantes d'une CCT ont l'obligation légale de veiller à l'observation de la convention, selon l'art. 357a al. 1 CO. Cette disposition leur impose de veiller à l'observation de la convention et d'intervenir auprès de leurs membres en usant, au besoin, des moyens que leur confèrent leurs statuts et la loi. L'obligation de faire observer la convention a été décrite dans le message relatif à l'entrée en vigueur de la LECCT comme

« consistant positivement, dans l'obligation d'exécuter et, négativement, dans l'obligation de maintenir la paix du travail »[28].

En cas d'extension de la CCT, la LECCT[29] prescrit également une obligation d'assurer l'égalité de traitement entre les entreprises et travailleurs signataires et les entreprises et travailleurs dits « dissidents » par la Commission paritaire. Cette condition est indispensable à la déclaration d'extension de la CCT[30]. L'obligation légale de traiter les données sensibles nécessaires à l'exécution de la convention s'appliquent par conséquent également à la Convention collective étendue par Arrêté fédéral. Une décision de l'Obergericht du canton de Lucerne déduit également de l'art. 4 al. 1 LECCT une « obligation de tolérer un contrôle pour les dissidents »[31]. Cela justifie, à notre sens, le fait que la commission paritaire ne soit pas soumise à l'obligation de déclarer les fichiers de données qu'elle traite dans le but de l'application de la CCT.

Une expertise du Préposé à la protection des données de 2001 tranche la question du point de vue de la communication de données : « Une base juridique qui prévoit explicitement la communication de données des travailleurs à des comités mixtes n'existe pas ». Nous comprenons cette prise de position par le trop large champ d'application de l'obligation de veiller à la bonne application des CCT exposée aux paragraphes précédents.

3. L'intérêt public prépondérant

En l'absence d'une base légale expresse, le motif justificatif pertinent pour la réception et le traitement de données par une commission paritaire est l'intérêt public prépondérant au contrôle de l'application de la LECCT.

a) L'intérêt public

Le rapport d'activité du Préposé fédéral à la protection des données(ci-après : le Préposé) pour la période 1998/1999 confirme l'existence d'un intérêt public justifiant l'activité des commissions paritaires dans le cadre de la pesée des intérêts en cause dans la consultation des documents nécessaires au contrôle de l'application d'une convention collective de travail; la pesée des intérêts est clairement exprimée par le Préposé de la manière suivante : « l'intérêt à la protection de la personnalité d'une pluralité de travailleurs l'emporte sur l'intérêt d'une seule entreprise à maintenir confidentielles ses données de gestion de salaires[32] ». Le Préposé en conclut que « lors de l'exécution du contrôle des livres de

28 Message LECCT, FF 1954 I 125, p. 162.
29 Art. 5 al. 1 LECCT.
30 Art. 2 al. 4 LECCT.
31 Décision de l'Obergericht du canton de Lucerne du 18 juillet 1989, *in* : LGVE 1989 I N° 15, p. 36.
32 PFPDT, Rapport 1998/1999, p. 66.

salaires, les employeurs ne peuvent donc pas refuser de transmettre les documents nécessaires au contrôle en se basant sur la protection des données »[33].

Le Tribunal administratif fédéral a également fait mention de l'intérêt public de l'activité de contrôle des commissions paritaires, et donc de leur accès aux données rendant ce contrôle possible dans un arrêt du mois de juin 2014[34]. Si l'arrêt ne porte pas directement sur un contrôle CCT, il concerne la demande formulée par l'association « Fonds paritaire d'application, de formation et social pour le secteur de la location de services » à la SUVA d'une liste des entreprises actives dans la location de services et dont le chiffre d'affaires dépasse un million deux cent mille francs. Ce montant correspond au chiffre d'affaires minimal prévu par la nouvelle CCT location de services. La demande faite à la SUVA vise donc à identifier quelles sont les entreprises de location de service susceptibles d'y être assujetties. La SUVA est, du point de vue de la LPD, une autorité fédérale au sens l'art. 19 al. 1bis LPD. Le Tribunal administratif fédéral met donc en balance l'intérêt de l'association « Fonds paritaire » à faire appliquer la CCT location de services à toutes les entreprises entrant dans son champ d'application face à l'intérêt des entreprises assurées auprès de la SUVA à garder confidentielles ces données. Il est intéressant de reprendre l'entier de la définition développée par le Tribunal administratif fédéral de l'intérêt public à l'accès aux données pour assurer le respect d'une CCT :

« Afin que les buts d'intérêt public puissent également être atteints, une mise en application rigoureuse ainsi que le respect généralisé des dispositions de la CCT par les entreprises qui y sont soumises, sont nécessaires, à la suite de la déclaration de force obligatoire générale. Partant, les recourants font à juste titre valoir que la mise en œuvre d'une CCT répond à un intérêt public. La garantie de la paix du travail, la protection des travailleurs et la prévention de la concurrence déloyale constituent des intérêts publics prépondérants et reconnus »[35].

b) L'intérêt privé des personnes contrôlées

Nous avons vu que l'intérêt public au traitement de données nécessaires par les organes paritaires chargés de l'exécution commune des CCT est développé de façon suffisamment claire. Il est avéré, quel que soit le biais par lequel l'entreprise et les travailleurs qu'elle emploie se voient appliquer la CCT : l'adhésion à l'association, la signature individuelle ou par le biais d'une extension. La condition posée par la LPD pour lever l'illicéité d'un traitement de données est bien l'existence d'un intérêt public, mais ce dernier doit également être prépondérant à l'intérêt privé du titulaire des données. Nous avons

33 PFPDT, Rapport 1998/1999, p. 66.
34 ATAF 2014/42 du 6 juin 2014, *in* : JdT 2015 I262.
35 ATAF 2014/42 du 6 juin 2014, c. 7.4.2., *in* : JdT 2015 I262.

recherché dans quelle mesure l'intérêt privé d'un employeur à refuser l'accès à l'organe paritaire avait déjà été mentionné dans la doctrine et la jurisprudence.

Le Préposé fédéral à la protection des données reconnaît un intérêt privé à l'employeur à maintenir confidentielles ses données de gestion de salaires dans le rapport précédemment cité[36]. HÄBERLI reconnaît également à l'employeur un « intérêt digne de protection à la confidentialité de la structure salariale de son entreprise »[37].

L'existence de ces intérêts n'est pas remise en question ; c'est seulement en comparaison avec l'intérêt public que représente la bonne application des conventions collectives de travail que celui-ci ne suffit plus à justifier le refus de laisser la commission paritaire traiter les données nécessaires. Nous exposerons au point III.4. ci-dessous en quoi cette primauté de l'intérêt public peut être tempérée par l'application des principes généraux de la protection des données, et, au point IV, en quoi l'art. 357b CO n'est pas supposé empêcher la collaboration de l'employeur à la procédure de contrôle. Ces considérations valent pour l'employeur qui cherche à éluder le contrôle CCT parce qu'il ne respecte pas les conditions minimales de travail et de salaire que celle-ci prévoit.

Lorsque la personne contrôlée essaye de se soustraire au contrôle de l'application de la CCT par une commission paritaire, on ne lui reconnaît plus cet intérêt digne de protection : le Tribunal fédéral a par exemple été saisi par une entreprise d'un recours contre une sentence arbitrale du Tribunal Arbitral du Gros œuvre du canton de Genève, laquelle confirmait une peine conventionnelle pour non-envoi de documents requis. Le Tribunal fédéral qualifie le recourant de « malvenu à se plaindre d'avoir été sanctionné alors qu'il lui aurait suffi de prêter son concours à la [commission paritaire genevoise du gros œuvre] et de répondre aux questions de cette dernière pour obtenir rapidement une clarification de sa situation juridique et, le cas échéant, la constatation formelle de son non-assujettissement aux conventions nationale et genevoise du gros œuvre »[38].

Dans l'arrêt du Tribunal administratif fédéral précédemment cité, il n'est reconnu « aucune protection aux entreprises qui se soustraient sciemment à l'application de la CCT – dont la mise en œuvre répond à des objectifs d'intérêt public – alors même qu'elles remplissent les critères de soumission »[39]. Le Tribunal administratif fédéral ne reconnaît également pas d'autres mesures que la transmission de la liste directement à l'instance paritaire responsable de l'action de la CCT location de service, au motif que « ce sont précisément les entreprises qui ne respectent pas la CCT qui, dans le futur, ne communiqueront pas aux

36 PFPDT, Rapport 1998/1999, p. 66.
37 HÄBERLI, N 45 *ad* art. 357b CO, p. 284.
38 TF 4A_67/2013 du 1er juillet 2013.
39 ATAF 2014/42 du 6 juin 2014, c. 7.4.3, *in* : JdT 2015 I 262.

organes d'exécution de la CCT des informations utilisables, respectivement des informations véridiques concernant leur masse salariale »[40].

4. Le respect des principes généraux de la LPD

Comme expliqué dans le cadre de l'intérêt public, l'existence d'un motif justificatif au traitement des données d'une entreprise et des travailleurs qu'elle emploie lève l'illicéité du traitement. Celui-ci reste conditionné aux principes généraux de la protection des données. La commission paritaire doit pour commencer organiser son système de gestion interne afin d'assurer l'exactitude des données traitées, ainsi que leur sécurité. Les deux principes qui seront importants dans le cadre du respect des principes généraux sont le principe de proportionnalité et le principe de finalité : les données en possession de la commission paritaire doivent pouvoir permettre le contrôle de l'application de la CCT, être conservées dans ce but, et il ne doit pas y avoir de mesure moins incisive qui permettrait également le contrôle CCT. L'expertise du Préposé conclut également qu'il n'existe pas d'alternative à l'examen des pièces fournies par l'entreprise pour effectuer un contrôle des conditions de travail et de salaire[41].

Les entreprises qui font l'objet d'un contrôle en sont directement informées[42] par l'association de contrôle ou la commission paritaire lors de la demande de documents ou l'inspection ; il appartient ensuite à l'employeur d'informer les travailleurs du contrôle[43].

Le Préposé reconnaît l'intérêt prépondérant à l'application des CCT, mais précise également que la prise de connaissance des documents doit se limiter aux données relatives aux travailleurs[44]. Selon ce même rapport, la saisie de données relatives à des tiers ne se justifie plus par un intérêt public.

B. Le renseignement de l'organe paritaire selon le contrat de travail

Cette partie de notre analyse vise à faire le lien entre le contrat de travail individuel régissant les rapports entre travailleurs et employeurs et le droit collectif qui s'applique à la relation entre la commission paritaire et les employeurs et travailleurs assujettis. Si la

---

40 ATAF 2014/42 du 6 juin 2014, c. 7.4.4, *in* : JdT 2015 I 262.

41 PFPDT, Rapport 1998/1999, p. 66 : « Der vom GAV verlangte Unterlagenkatalog wird für eine wirksame Lohnbuchkontrolle benötigt und ist zweck- und verhältnismässig ».

42 Cf. le devoir d'informer prévu par l'art. 14 LPD.

43 HÄBERLI, N 45 *ad* art. 357b CO, p. 284, commentaire de l'expertise du PFPDT, *in* : JAAC 65.99 (voir *infra*.). Le rapport de l'activité du Préposé pour les années 1998/1999 mentionne que les travailleurs doivent être informés, mais sans préciser par qui.

44 PFPDT, Rapport 1998/1999, p. 66.

commission paritaire peut justifier son action par un intérêt public généralement prépondérant comme exposé ci-dessus, il faut également examiner si la transmission de documents à une commission paritaire par une des parties au contrat individuel de travail peut constituer une violation de ses obligations envers l'autre partie, et si cette violation peut être justifiée.

1. L'article 328b CO

L'art. 328b CO autorise l'employeur à traiter les données de son employé dans le strict cadre de l'aptitude du travailleur à remplir son emploi ou de la nécessité à l'exécution du contrat de travail. Un avis de droit de 2001 du Préposé considère que la communication de données à une commission paritaire repose sur une relation de droit indépendante de l'exécution du contrat individuel de travail au sens de l'art. 328b CO[45]. Les règles générales de la LPD s'appliqueront donc à la communication de données à la commission paritaire, comme le prescrit l'art. 328b CO 2e phrase.

Il est important de rappeler que l'article 328b CO constitue une disposition relativement impérative selon l'art. 362 CO, c'est-à-dire à laquelle il ne peut être dérogé au détriment du travailleur[46]. La signature d'une CCT en défaveur des travailleurs sur le point de la protection des données ne serait donc pas admissible[47]. HÄBERLI prescrit, comme déjà mentionné, qu'il appartient à l'employeur d'informer les travailleurs du contrôle[48]. L'expertise du Préposé considère que l'adhésion à une partie contractante à la CCT correspond à un engagement à en respecter les dispositions normatives, mais aussi à en accepter les dispositions relatives au contrôle. Si un consentement au traitement de données existe pour les travailleurs signataires de la CCT, il est difficile de déduire un consentement pour les travailleurs auquel la CCT s'applique par extension selon la LECCT. Les motifs justificatifs déjà mentionnés peuvent cependant justifier la communication de données concernant les travailleurs par l'employeur à une commission paritaire dans le but d'un contrôle du respect des conditions de travail et de salaire selon une CCT étendue.

2. L'article 321 CO

Le travailleur doit respecter son devoir de fidélité au sens de l'art. 321a al. 1 et 4 CO, et est notamment tenu à une obligation générale de garder le secret. L'aspect négatif du devoir de fidélité est le devoir de « s'abstenir de léser l'employeur dans ses intérêts

45 PFPDT, Expertise, ch. 4.

46 DUNAND, N 11 *ad* art. 328b CO, p. 322 ; Message LPD, FF 1988 II 421 (494) ; PFPDT, Guide, N 2.2.2, p. 6.

47 PFPDT, Expertise, ch. 3.

48 PFPDT, Expertise, ch. 3 ; HÄBERLI, p. 284.

légitimes et éviter, en particulier, tout ce qui pourrait lui causer un dommage économique[49] ». Ce devoir trouve notamment deux limites qui, à notre sens, permettent de justifier la communication de données à une commission paritaire par le travailleur : d'une part, les intérêts de l'employeur à ne pas respecter une convention collective de travail ne sont pas considérés comme légitimes, comme nous l'avons conclu ci-dessus, et d'autres part, le devoir de fidélité du travailleur trouve ses limites lorsque le travailleur fait valoir ses propres intérêts dignes de protection à transmettre des renseignements[50]. L'intérêt des travailleurs à la bonne application de la CCT a déjà été établi ci-dessus. Le renseignement d'une commission paritaire dans le cadre du contrôle CCT n'est par conséquent, selon notre compréhension, pas une violation des obligations du travailleur. Un licenciement basé sur ce motif serait probablement considéré comme abusif au sens de l'art. 336 al. 1 lit. c CO.

IV. Le refus de transmettre les données nécessaires au contrôle

Une des difficultés pratiques majeures rencontrées par les commissions paritaires dans leurs activités de contrôle est le refus de collaboration à la procédure de la part des personnes contrôlées. Ce point traitera des différents instruments que peuvent utiliser les commissions paritaires pour réagir à cette absence de collaboration :

A. La sanction de la non-collaboration par une peine conventionnelle

La commission paritaire peut prononcer une peine conventionnelle envers l'entreprise qui se dérobe à ses obligations de renseignement : l'obligation de renseigner doit être prévue dans la CCT[51]. La Cour civile du canton du Jura a dû se prononcer en 2015 sur une sanction de non-collaboration à la procédure de contrôle prononcée par la commission paritaire du Second œuvre jurassienne envers une entreprise active dans la location de service. Elle a

---

49 DUNAND, N 14 *ad* 321*a* CO, p. 57 et les références citées.

50 STAEHELIN, N 8 *ad* art. 321a CO, p. 83 ; REHBINDER/STÖCKLI, N 9 *ad* art. 321a CO, p. 134.

51 Par exemple :
Art. 47 al. 3 CCT SOR : Les représentants délégués par les Commissions professionnelles paritaires cantonales sont autorisés à entrer dans les entreprises soumises à la présente convention. L'employeur est tenu de se présenter devant eux et de leur permettre l'accès à l'entreprise, respectivement l'employeur a l'obligation de présenter tous documents et informations utiles.

confirmé le motif et le montant de la peine conventionnelle : « Face à l'obstination de la recourante de refuser de collaborer durant près de deux ans, on ne saurait considérer que l'amende de CHF 5'000.- est excessive, de sorte qu'il n'y a pas lieu de la réduire »[52].

Le Tribunal fédéral s'est également prononcé, cette fois saisi d'un recours contre une sentence arbitrale, sur le principe d'une peine prononcée par la Commission paritaire genevoise du gros œuvre dans un cas de « non-envoi de document requis » envers une entreprise dans le cadre d'un contrôle d'assujettissement à la Convention nationale du secteur principal de la construction envers une entreprise active dans le secteur du second œuvre, contrôlée effectuant des travaux de gros œuvre ; le Tribunal a également reconnu le motif et le montant de la peine conventionnelle[53].

Les deux peines conventionnelles confirmées par les arrêts ci-dessus concernaient d'une part une entreprise dissidente, et d'autre part une entreprise active dans la location de service. Cela appuie la légitimité des commissions paritaires à prononcer des sanctions contre l'absence de collaboration d'une entreprise, non seulement contre les entreprises et travailleurs signataires, mais aussi envers les entreprises qui ne sont pas assujetties à la CCT par choix. La peine conventionnelle permet de sanctionner le refus de collaborer, mais non d'obliger l'entreprise ou le travailleur à renseigner la commission paritaire, si ce n'est indirectement.

B. La désignation d'un organe spécial de contrôle

L'art. 6 LECCT offre aux entreprises dissidentes[54] la possibilité de demander en tout temps à l'autorité compétente la désignation d'un organe spécial de contrôle. Le message de 1954 relatif à la LECCT désigne cette possibilité par « l'inadmissibilité de soumettre un dissident contre sa volonté au contrôle des organes des associations »[55]. RONCORONI tempère ce droit des dissidents en rappelant qu'il est également soumis à la réserve de l'abus de droit[56].

Les personnes ayant qualité pour demander la désignation d'un organe spécial de contrôle sont les entreprises dissidentes, et les entreprises locataires de service, par application

---

52 Arrêt du Tribunal cantonal du canton de Jura du 14 janvier 2015, c. 7.5, *in* : RJJ 2015 p. 217.

53 TF 4A_67/2013 du 1er juillet 2013, c. 3.2.2. : « N'ayant pas pu obtenir du recourant la collaboration requise, elle a utilisé la sanction conventionnelle que constitue l'amende afin de l'y contraindre. On ne voit pas que le Tribunal arbitral ait versé dans l'arbitraire en entérinant pareille sanction. ».

54 Les entreprises dissidentes sont celles à qui la CCT s'applique par le biais d'un Arrêté administratif d'extension selon le LECCT. La traduction allemande est « Aussenseiter ».

55 Message LECCT, FF 1954 I 125 (176).

56 RONCORONI, N 207 *ad* 6 LECCT, pp. 449-450.

analogique inscrite à l'article 48 al. 4 OSE. Ce droit n'est pas ouvert aux entreprises signataires[57].

Depuis le 1er juin 2004, la possibilité de demander la désignation d'un organe spécial de contrôle est également ouverte aux parties à la convention, lorsqu'un employeur ou un travailleur auquel la convention est étendue refuse de se soumettre au contrôle de l'organe paritaire, par l'art. 6 al. 1 *in fine* LECCT. Le but de la désignation d'un organe spécial de contrôle, selon le message de 1999, est de « contraindre un employeur à tolérer un contrôle afin de déterminer si la CCT est respectée, ou si, dans le cas contraire, les travailleurs pourraient émettre des prétentions »[58]. Permettre aux parties contractantes de demander également cette désignation comble une lacune de la loi[59]. HÄBERLI rappelle que « [l]es litiges portant sur l'existence d'un droit de contrôler, dont le principe serait contesté ne sont pas tranchés par "l'autorité compétente selon 6 LECCT", mais par le juge civil ; aussi l'al. 1 concerne-t-il les cas où le dissident ne conteste pas le droit de contrôler en tant que tel, mais refuse l'organe de contrôle prévu par la CCT »[60]. L'art. 6 LECCT ne résout donc pas non plus la situation dans laquelle une entreprise refuse le principe d'un contrôle CCT, et pas seulement la compétence de la commission paritaire.

C. Le recours au juge civil

Il existe peu de littérature et de jurisprudence portant spécialement sur la production des documents nécessaires au contrôle CCT sur demande de la commission paritaire. Ces questions se règlent, en Suisse romande particulièrement, devant des tribunaux arbitraux spécialisés ou des juridictions spécialisées pour le traitement des conflits collectifs de travail[61]. Le système de l'arbitrage nécessite la reconnaissance de la compétence de l'arbitre par la partie qui refuse la collaboration à la procédure. Les instances spécialisées interviennent au préalable comme autorité de conciliation. Ces outils ne suffisent souvent pas à obtenir les documents nécessaires au contrôle. C'est pourquoi une requête en procédure civile est, dans certains cas, le seul moyen d'obtenir les documents.

Nous examinerons d'abord la qualité pour agir des commissions paritaires de manière générale, avant de développer le cas de la requête en procédure applicable aux cas clairs,

---

57 Le Préposé avait mentionné, dans l'expertise de 2001 précitée, qu'il serait souhaitable que cette possibilité soit ouverte également aux entreprises signataires. La proposition n'a pas été suivie par une modification de la loi.

58 Message LDét, FF 1999 5540 (5702).

59 TRUNIGER, N 7 *ad* art. 357b, p. 859.

60 RONCORONI, N 213 *ad* art. 6 LECCT, p. 451, et les références citées.

61 Par exemple : Chambre des relations collectives de travail du Canton de Genève (CRCT).

puis présenterons rapidement les types d'actions pour les situations juridiques ne répondant pas aux conditions de l'art. 257 CPC.

1. La qualité pour agir d'une commission paritaire

La commission paritaire qui souhaite obtenir les documents nécessaires à l'exécution du contrôle par le biais d'une requête devant les tribunaux civils doit disposer de la légitimation active pour agir. Cette question a longtemps été controversée ; la qualité pour agir des organes paritaires disposant de la personnalité juridique n'est aujourd'hui pas contestée[62]. DIETSCHY rappelle également que « rien n'empêche [les] membres de la commission paritaire d'agir comme représentants des associations signataires de la convention collective parties à la procédure »[63]. Il reste cependant nécessaire, pour la commission paritaire, d'apporter la preuve que ses statuts ou la CCT lui permettent d'agir en justice, et si la convention collective permet à la Commission paritaire d'agir en ce sens.

2. La requête en procédure applicable aux cas clairs

a) L'admissibilité d'une demande de production de document

L'art. 257 CPC prévoit l'application de la procédure sommaire à certaines conditions. Si le juge admet que la requête constitue un cas clair, il admet celle-ci et « accorde la protection demandée ; cette décision acquiert autorité et force de chose jugée »[64].

L'objet de la décision peut être une obligation de faire[65]. La commission paritaire peut donc, du point de vue de l'objet, déposer une requête pour obtenir la production des documents nécessaires au contrôle de la CCT. La requête doit cependant encore répondre aux deux autres conditions exigées par l'art. 257 al. 1 lit. a et b CPC : l'état de fait doit être non contesté ou susceptible d'être immédiatement prouvé, et la situation juridique doit être claire.

Le message du Conseil fédéral précise que la situation de fait doit être « établie sans peine »[66] ; la jurisprudence décrit le cas clair comme celui où « sur la base du dossier, le juge parvient à la conclusion que la demande est fondée et qu'un examen plus détaillé des objections avancées par le défendeur n'y changerait rien »[67]. DIETSCHY précise à ce sujet

62 ATF 134 III 541, c. 4.2.
63 DIETSCHY, N 74, p. 359.
64 HOFMANN/LÜSCHER, p. 342 ; Message CPC, FF 2006 6924 (6959).
65 HOHL, Procédure civile I, N 1655, p. 303.
66 Message CPC, FF 2006 6924 (6959).
67 ATF 38 III 620, c. 5.1.1, *in* : SJ 2013 I 283 (trad).

que « [l]es objections manifestement infondées ou dénuées de pertinence sur lesquelles il est possible de statuer immédiatement ne suffisent pas à exclure le cas clair »[68].

La situation de fait et de droit est claire, à notre sens, lorsque l'activité de l'entreprise qui ne collabore pas appartient au genre d'activité concerné par la CCT ou l'Arrêté fédéral d'extension, et que les travailleurs concernés appartiennent au champ d'application personnel de la CCT ou de l'Arrêt d'extension.

DIETSCHY présente le cas d'un travailleur réclamant la différence de salaire entre le salaire minimum obligatoire selon la CCT applicable à la branche et celui qui lui a effectivement été versé par l'employeur comme un cas clair si les pièces suivantes sont apportées : copie du contrat de travail, des fiches de salaires et des dispositions de la CCT applicable[69]. Cela signifie que l'application d'une CCT peut également être considérée comme un cas clair par le juge civil.

La procédure de l'art. 257 CPC était connue, dans certains cantons alémaniques, sous le nom de « Befehlsverfahren »[70]. C'était notamment le cas du canton de Luzern. Un arrêt de l'Obergericht lucernois du 18 juillet 1989[71] et en partie publié reprend les conditions de la qualité pour agir d'un organe paritaire dans le cadre d'une « Befehlsverfahren » accordée à un organe paritaire contre une entreprise dissidente faisant « obstruction » au contrôle de la CCT. L'Obergericht confirme la compétence de l'organe paritaire pour demander la protection dans les cas clairs, et reconnaît l'obligation de tolérer un contrôle CCT des dissidents en cas de convention étendue. L'argument avancé par l'entreprise décrivant le contrôle CCT comme une violation de l'art. 28 CC est également réfuté. L'Obergericht rejette donc le recours de l'entreprise dans l'ensemble de ses conclusions[72].

b) La motivation de la requête

La requête formulée par une commission paritaire à l'encontre d'une entreprise refusant de transmettre les documents demandés peut porter sur les deux obligations suivantes : l'obligation de remettre les documents nécessaires au contrôle et l'obligation de tolérer un contrôle sur place. La commission doit, dans sa requête, démontrer que l'entreprise est bien assujettie à la CCT. La liste des documents ou la description du contrôle que la commission souhaite faire tolérer à l'entreprise sont également à mentionner sur la requête.

---

68 ATF 38 III 620, c. 5.1.1, *in* : SJ 2013 I 283 (trad).

69 DIETSCHY, N 480, p. 235.

70 HOFMANN/LÜSCHER, p. 342.

71 Décision de l'Obergericht du canton de Lucerne du 18 juillet 1989, *in* : LGVE 1989 I N° 15, pp. 35-37.

72 Décision de l'Obergericht du canton de Lucerne du 18 juillet 1989, *in* : LGVE 1989 I No. 15, pp. 36 et 37.

Les bases légales et conventionnelles de la requête seront l'art.257 CPC, l'art. 357b CO, les articles de la CCT et du CO en rapport avec l'exécution commune, les statuts de la commission paritaire, voire même une procuration signée par les parties contractantes. Si l'entreprise n'est pas signataire, le requête devra également mentionner l'Arrêté d'extension de la CCT et la LECCT.

L'opportunité de demander la protection pour les cas clairs doit s'examiner au cas par cas : la condition de « situation juridique claire » peut ne pas être donnée selon la complexité de la structure de l'entreprise assujettie, ou si l'entreprise apporte des objections fondées à son assujettissement. L'Obergericht du Canton de Saint-Gall a déjà rejeté la protection pour les cas clairs dans un cas ou l'entreprise visée contestait son assujettissement[73]. Dans un autre domaine juridique, le Tribunal fédéral a déjà nié, dans un arrêt concernant l'information mutuelle des époux selon l'art 170 CC, le caractère liquide d'un cas en raison de l'étendue et la complexité des renseignements requis. Lorsque la commission paritaire réalise que le cas dépasse le cadre posé par l'art. 247 CPC, il est nécessaire de procéder par un autre moyen de droit.

3. Les autres requêtes

Lorsque la situation de fait ou de droit dépasse les cas d'application de l'art. 253 CPC, différentes voies de droit s'offrent aux commissions paritaires : DIETSCHY répertorie notamment deux possibilités : « [l]a prétention visant à la mise en place d'un contrôle » , dont « la valeur litigieuse devrait être estimée en fonction des montants vraisemblablement visés par la violation des dispositions de la CCT »[74] et « [l]a prétention en constatation de l'assujettissement à une CCT »[75] dont la valeur litigieuse doit être calculée « en fonction de l'intérêt de l'employeur à ne pas être assujetti à la CCT, c'est-à-dire du coût supplémentaire que l'application de celle-ci entraînerait pour l'entreprise […] »[76].

Si l'entreprise maintient son refus de collaborer à la procédure y compris devant le Tribunal civil, le message du CPC prévoit que le refus injustifié d'une partie est « sans conséquence disciplinaire ou pénal ni passible de contrainte »[77] ; le Tribunal doit, si une

---

73 Décision du Kantonsgericht St-Gall, Einzelrichter im Obligationenrecht BS.2014.7 du 13 octobre 2014.

74 DIETSCHY, N 717, p. 344 ; ATF 118 II 528, *in* : JdT 1993 I pp. 654 et 656.

75 Dietschy, N 717 et 718, p. 344.

76 DIETSCHY, N 717, p. 344 et les références citées.

77 Message CPC, FF 2006 6924 (6296).

partie refuse de collaborer sans motifs valable, en tenir compte lors de l'appréciation des preuves[78]. HALDY considère cette sanction comme procédurale[79].

Face à un refus total de transmettre des documents de la part de l'entreprise, il est difficile d'estimer la valeur litigieuse des prétentions de la commission paritaire. Il reste alors deux possibilités à examiner à notre sens : recourir à l'action échelonnée (Stufenklage), que HOHL définit comme une « action principale en paiement non chiffrée, accompagnée d'une demande accessoire préalable fondée sur un droit à la communication des renseignements et de pièces découlant du droit matériel »[80], ou l'action en preuve à futur, de l'art. 158 al. 1 lit b, lorsque la commission peut faire valoir un intérêt digne de protection.

Selon le Message, « la locution "intérêt digne de protection" implique que la preuve à futur puisse aussi servir à évaluer les chances d'obtenir gain de cause ou d'apporter une preuve[81] ». Le Tribunal fédéral prescrit cependant que « [l]a procédure de preuve à futur n'a, dans tous les cas, pas pour objet d'obtenir qu'il soit statué matériellement sur les droits ou obligations des parties […][82] ».

Le critère commun entre l'action échelonnée, la preuve à futur et la requête en protection dans la procédure pour les cas clairs reste un droit matériel de la commission paritaire à obtenir les documents. HOHL est d'avis que « lorsque le défendeur conteste l'existence même du droit aux renseignements, une action et une décision sur le bien-fondé de ce droit matériel sont nécessaires[83] ». Nous rejoignons cet avis, et doutons par conséquent de l'application de la preuve à futur dans le cas d'un refus de contrôle CCT.

V. Conclusion

Les commissions paritaires ont un rôle à jouer dans l'organisation du marché du travail suisse. L'intérêt public à effectuer ces contrôles, on l'a vu plus haut, n'est pas contesté. Il est cependant toujours difficile d'obtenir les documents nécessaires au contrôle. Le dernier point de cet article a essayé de référencer les moyens à disposition de la commission paritaire de faire face à cette difficulté. L'action de la commission paritaire étant

78 Art. 164 CPC.
79 HALDY, p. 51.
80 HOHL, Procédure civile I, N 502, p. 93.
81 Message CPC, FF 2006 6924 (6296).
82 ATF 142 III 40, c. 3.1.3.
83 HOHL, Procédure civile I, N 504, p. 94.

notamment motivée par un intérêt public, mais régie par le droit privé, ces moyens peuvent en pratique, manquer de réactivité.

Plus généralement, afin de conserver leur légitimité et rester les représentantes de l'intérêt public que constituent la majorité des travailleurs et des employeurs soumis à la convention, les commissions paritaires doivent également considérer, dans leur travail d'application, les principes de la protection des données. L'adoption d'un règlement interne concrétisant ceux-ci dans le cas particulier de l'activité d'une CCT peut les soutenir dans cette obligation[84].

Bibliographie

AUBERT GABRIEL, Conventions collectives de travail : évolution dans la perspective de l'EEE, *in* : L'avenir des relations sociales dans l'Espace économique européen : symposium tenu à Lausanne le 4 septembre 1992, Lausanne 1992, pp. 22-28.

BAERISWYL BRUNO, Commentaire de l'art. 10a LPD, *in* : Bruno Baeriswyl/Kurt Pärli (éds.), Datenschutzgesetz (DSG) – Handkommentar, Berne 2015.

BRUCHEZ CHRISTIAN, Commentaire de l'art. 357b CO, *in* : Jean-Philippe Dunand/Pascal Mahon (éds.), Commentaire du contrat de travail, Berne 2013.

BRUCHEZ CHRISTIAN, Commentaire de l'art. 356 CO, *in* : Arthur Andermatt/Doris Bianchi/Christian Bruchez et al. (éds.), Droit collectif du travail, Bâle 2010, pp. 161-197 (cité : BRUCHEZ, Droit collectif).

CONSEIL FÉDÉRAL, Message concernant la loi fédérale sur la protection des données (LPD) du 23 mars 1988, FF 1988 II 421 (cité : Message LPD).

CONSEIL FÉDÉRAL, Message relatif à la loi fédérale permettant d'étendre le champ d'application de la convention collective de travail du 19 janvier 1954, FF 1954 I 125 (cité : Message LECCT).

CONSEIL FÉDÉRAL, Message relatif à la loi fédérale sur les mesures d'accompagnement applicables aux travailleurs détachés et aux contrôles salaires minimaux prévus par les contrats-types de travail (Loi sur les travailleurs détachés, LDét) du 8 octobre 1999, FF 1999 5540 (cité : Message LDét).

CONSEIL FÉDÉRAL, Message relatif au Code de procédure civile suisse (CPC) du 28 juin 2006, FF 2006 6924 (cité : Message CPC).

DIETSCHY PATRICIA, Les conflits de travail en procédure civile Suisse, thèse, Neuchâtel/Bâle 2011.

DUNAND JEAN-PHILIPPE, Commentaire des art. 321a et 328b CO, *in* : Jean-Philippe Dunand/Pascal Mahon (éds.), Commentaire du contrat de travail, Berne 2013.

[84] Par exemple : les dispositions du règlement de procédure de la Commission paritaire centrale suisse d'application de la convention nationale du secteur de la construction relative à la protection des données.

GROUPE DE TRAVAIL « BESOINS D'AMÉLIORATION DE L'EXÉCUTION ET DE LA LUTTE CONTRE LES ABUS DANS LE CADRE DES MESURES D'ACCOMPAGNEMENT », Rapport à l'attention du Conseil fédéral du 23 novembre 2016 (cité : Rapport du groupe de travail FlaM).

HÄBERLI, CHRISTOPH, Commentaire de l'art. 357b CO, *in* : Arthur Andermatt/Doris Bianchi/Christian Bruchez et al. (éds.), Droit collectif du travail, Bâle 2010, pp. 265-292.

HALDY JACQUES, La nouvelle procédure civile Suisse, Bâle 2009.

HOFMANN DAVID/LÜSCHER CHRISTIAN, Le code de procédure civile, 2e édition, Berne 2015.

HOHL FABIENNE, Procédure civile, tome I, 2e édition, Berne 2016 (cité : HOHL, Procédure civile I).

HOHL FABIENNE, Procédure civile, tome II, 2e édition, Berne 2010 (cité : HOHL, Procédure civile II).

KULL, MICHAEL, Arbeitsvermittlungsgesetz (AVG) – Handkommentar, Berne 2014.

MATILE PIERRE/ZILLA JOSÉ/STREIT DAN, Travail temporaire – Commentaire pratique des dispositions fédérales sur la location de services (art. 12-39 LSE), Neuchâtel 2010.

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

PRÉPOSÉ FÉDÉRAL À LA PROTECTION DES DONNÉES ET À LA TRANSPARENCE, Guide pour le traitement des données personnelles dans le secteur du travail, Berne 2014, (cité : PFPDT, Guide).

PRÉPOSÉ FÉDÉRAL À LA PROTECTION DES DONNÉES ET À LA TRANSPARENCE, Rapport d'activités no 6 (1998/1999), Berne 1999 (cité : PFPDT, Rapport 1998/1999).

PRÉPOSÉ FÉDÉRAL À LA PROTECTION DES DONNÉES ET À LA TRANSPARENCE, Expertise du 11 juillet 2001, *in* : JAAC 65.99 (cité : PFPDT, Expertise).

REHBINDER MANFRED/STÖCKLI JEAN-FRITZ, Art. 319-330b OR : Der Arbeitsvertrag : Der Einzelarbeitsvertrag – Berner Kommentar, Berne 2010.

RONCORONI GIACOMO, Commentaire des art. 1 à 21 LECCT, *in* : Arthur Andermatt/Doris Bianchi/Christian Bruchez et al. (éds.), Droit collectif du travail, Bâle 2010.

SECRÉTARIAT D'ETAT À L'ECONOMIE (SECO), Directive sur l'extension du champ d'application des conventions collectives de travail : directives relatives aux contributions, état en novembre 2014, Berne 2014 (cité : SECO, Directive sur les contributions professionnelles).

SECRÉTARIAT D'ETAT À L'ECONOMIE (SECO), Directive « Procédure modèle sur l'exécution des mesures d'accompagnement par les commissions paritaires (CP) », état au 10 novembre 2015, Berne 2015 (cité : SECO, Directive Procédure modèle).

STAEHELIN ADRIAN, Art. 319-330a OR. Der Arbeitsvertrag – Zürcher Kommentar, Zurich 2015.

TRUNIGER PHILIPP, Commentaire de l'art. 357b CO, *in* : Jolanta Kren Kostkiewicz/Peter Nobel/Ivo Schwander/Stephan Wolf (éds.), Schweizerisches Obligationenrecht – OR Handkommentar, Berne 2009.

WYLER RÉMY/HEINZER BORIS, Droit du travail, 3e édition, Berne 2014.

Ouvrages parus dans la collection

Volume 10

Jean-Philippe Dunand / Pascal Mahon (éds)
La protection des données dans les relations de travail,
CERT 2017

Volume 9

Héloïse Rosello
Les influences du droit privé du travail sur le droit de la fonction publique,
CERT 2016

Volume 8

Jean-Philippe Dunand / Pascal Mahon / Stéphanie Perrenoud (éds)
Le droit de la relation de travail à la croisée des chemins : Convergences et divergences entre le droit privé du travail et le droit de la fonction publique – Droit suisse et droit comparé, CERT 2016

Volume 7

Jean-Philippe Dunand / Karine Lempen / Pascal Mahon (éds)
L'égalité entre femmes et hommes dans les relations de travail, CERT 2016

Volume 6

Jean-Philippe Dunand / Pascal Mahon (éds)
Conflits au travail, CERT 2015

Volume 5

Jean-Philippe Dunand / Pascal Mahon (éds)
Internet au travail, CERT 2014

Volume 4

Béatrice Despland
L'obligation de diminuer le dommage en cas d'atteinte à la santé – son application aux prestations en espèces dans l'assurance-maladie et l'assurance-invalidité,
CERT 2011

Volume 3

Marie Deveaud-Plédran
Le harcèlement dans les relations de travail, CERT 2011

Volume 2

Pierre Matile / José Zilla
Travail temporaire – Commentaire pratique des dispositions fédérales sur la location de service (art. 12-39 LSE), CERT 2010

Volume 1

Christian Flueckiger
Dopage, santé des sportifs professionnels et protection des données médicales, CERT 2008