Internet au travail

Jean-Philippe Dunand
Pascal Mahon

Volume 5

Jean-Philippe Dunand | Pascal Mahon (éd.)

Carole Aubert | Daniela Cerqui
Bertil Cottier | Régine Delley
Jean-Philippe Dunand | Sébastien Fanti
Christian Flueckiger | Sylvain Métille
Geneviève Ordolli | Vincent Salvadé
Olivier Subilia | Nathalie Tissot

Internet au travail

Préface de Laurent Kurth
Président du Conseil d'Etat neuchâtelois

Centre d'étude des relations de travail

Schulthess
ÉDITIONS ROMANDES
§ 2014

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.

ISBN 978-3-7255-6991-5

www.schulthess.com

Avant-propos

La technologie devance toujours le droit ! L'utilisation d'Internet au travail, très fréquente dans la plupart des entreprises et administrations de notre pays, reste soumise à un régime juridique lacunaire et incertain. A défaut de dispositions légales spécifiques, on applique les règles ordinaires du droit suisse.

Pour tenter de répondre aux principales questions juridiques concernant Internet au travail, un colloque a été organisé le 13 février 2014 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). L'ouvrage comprend les actes du colloque sous la forme de dix articles rédigés par douze contributrices et contributeurs suisses romands, actifs dans l'enseignement et/ou la pratique du droit du travail et du droit des nouvelles technologies.

Nos 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 Joanna David (cheffe de projet auprès de Schulthess éditions romandes), Kim Dreyer (Maîtrise en droit de l'Université de Genève) et Sylvia Staehli (assistante de direction à l'Université de Neuchâtel), pour leur collaboration efficace à l'édition de l'ouvrage, ainsi qu'à Mesdames Carole Aubert (avocate à Neuchâtel), Régine Delley (avocate, responsable du service juridique de la Chambre neuchâteloise du commerce et de l'industrie) et Anouk Gillabert (collaboratrice administrative à l'Université de Neuchâtel), pour leur précieuse aide à l'organisation du séminaire. Nous tenons enfin à remercier également Messieurs Pascal Mahon, vice-recteur de l'Université de Neuchâtel et codirecteur du CERT, qui a assuré la présidence du séminaire, et Laurent Kurth, président du Conseil d'Etat neuchâtelois, qui nous a fait l'honneur d'ouvrir le séminaire et de rédiger la préface de l'ouvrage.

Prof. Jean-Philippe Dunand,
codirecteur du CERT

Préface

Une administration virtuelle en marche !

Internet ou le réseau des réseaux est devenu en une décennie un vecteur de communication essentiel, rapide et aisément accessible. Un vecteur de communication qui a, pour beaucoup d'entre nous, progressivement bouleversé nos manières de communiquer mais aussi nos modes de travail.

L'Etat de Neuchâtel n'échappe pas aux évolutions liées aux nouvelles technologies de l'information. Comme toute collectivité publique, il s'y adapte constamment et tente de les anticiper en exploitant au mieux les outils à disposition à la fois pour son administration, mais aussi pour l'ensemble de ses usagers et la population. Tout en restant conscient qu'Internet crée un environnement très ouvert et fortement sollicité, avec ses avantages mais également ses risques.

Avec Internet, les notions de temps et d'espace ont été complètement relativisées, voire gommées, tant dans nos vies privées que sur nos lieux de travail : le courrier qui mettait trois jours à arriver de Berne est devenu le courriel envoyé et reçu instantanément, une insomnie en milieu de nuit peut être valorisée pour régler quelques affaires via la toile sans se soucier de la disponibilité de son interlocuteur et un déplacement à l'étranger n'empêche plus de traiter les affaires courantes ; les e-mails privés ou professionnels sont aussi disponibles sur l'ordinateur du bureau que celui de la maison et les journaux écrits ou audio-visuels se retrouvent tous sur le réseau en un clic de souris. Ainsi les parts du temps dédiées au travail et à la vie privée s'entremêlent et posent la question de la surveillance sur le lieu de travail. Faut-il contrôler ? Faut-il limiter les accès ? Comment ? Qui ? Jusqu'où ?

Dès l'ouverture généralisée d'Internet aux collaborateurs, deux mesures concrètes ont été mises en place pour en cadrer son usage au sein de l'administration cantonale neuchâteloise : d'une part des directives d'utilisation à l'usage des collaborateurs ont été introduites, avec des objectifs de protection des systèmes, de restriction à l'usage de l'infrastructure professionnelle à des fins privées et de limitation du temps « non travaillé » à la place de travail ; d'autre part, le service informatique de l'Etat de Neuchâtel a installé des filtres limitant l'accès à des sites non désirés (pornographie, jeux, violence, etc.). C'est donc une solution pragmatique et relativement simple à réaliser qui a été choisie, basée également sur la confiance que l'employeur doit placer en ses collaborateurs et dans le contrôle hiérarchique et/ou ponctuel mis en place.

Cet assouplissement de la frontière entre vie privée et vie professionnelle offre aussi des possibilités très intéressantes dans le cadre d'une politique des ressources humaines flexible et ouverte aux nouvelles formes de travail. Grâce à des connexions Internet sécurisées VPN, l'administration peut offrir des environnements de travail au domicile de la personne et lui permettre d'effectuer son activité en partie chez elle. A l'heure actuelle, le télétravail est déjà implanté dans notre administration pour des temps partiels, soit pour des personnes qui jouissent d'une autonomie d'organisation suffisante ou celles qui travaillent sur des dossiers standardisés, comme par exemple les taxateurs fiscaux : grâce à cet environnement électronique sécurisé, ils traitent les déclarations – désormais elles aussi électroniques – à domicile et réalisent les objectifs visés tout en gérant plus souplement leurs horaires. Enfin, grâce à la vidéoconférence et à la téléphonie mobile gratuite, on en vient à créer des environnements collectifs de travail virtuels !

Internet, c'est aussi la naissance du « bureau sans papier » dans bien des secteurs de l'administration, de l'enseignement mais aussi pour les autorités politiques. Ainsi en 2013, alors que le Grand Conseil se dotait d'une infrastructure informatique sécurisée propre et passait au vote électronique, les membres du Conseil d'Etat ont abandonné leurs piles de dossiers pour se doter d'ordinateurs-tablettes et passer au « gouvernement sans papier ». Cette petite réforme peut paraître anodine. Elle a néanmoins modifié du jour au lendemain des modes de fonctionnement et des pratiques de travail. Et a amené son lot de questions pratiques dans l'organisation du travail, dont celles liées à une nouvelle gestion des dossiers au sein de l'administration, à la circulation de l'information entre les services et les autorités, au classement et à l'archivage électroniques.

En quelques années, Internet a ainsi facilité les échanges d'informations et les activités au sein de l'administration cantonale. Il a aussi été un vecteur essentiel de partage d'informations entre les collectivités publiques et avec de nombreux acteurs de la vie active, comme par exemple les notaires qui, de leur cabinet, ont directement accès à toute une série de registres (registre du commerce, foncier, des poursuites, ou encore le registre suisse des certificats de décès, etc.) et informations essentielles à leurs activités (p. ex. données concernant le territoire).

Pour l'Etat de Neuchâtel, la plus importante concrétisation et expression de ce fabuleux vecteur de communication est sans aucun doute le guichet sécurisé unique (GSU), infrastructure de communication entre toutes les administrations publiques neuchâteloises et leurs usagers, personnes privées ou personnes morales. Avec le GSU, l'administration virtuelle neuchâteloise est en marche : plus de 200 prestations sont déjà accessibles sur cette plate-forme mise en exploitation depuis 2005. Les Neuchâteloises et Neuchâtelois peuvent y voter (Neuchâtel est le canton qui a effectué le plus de votations en ligne en Suisse, dont les élections cantonales de 2013), suivre leur compte courant fiscal, obtenir

un extrait de poursuites, modifier un rendez-vous pour l'expertise de leur véhicule et, pour les employés de l'administration, obtenir leur fiche de paie. En 2013, pas moins de 800'000 cyber-prestations ont été offertes sur le Guichet unique. Et ce sans contrainte liée aux heures d'ouverture des bureaux et sans nécessité de se déplacer pour le citoyen-usager !

Dans un avenir proche, nous avons l'intention d'élargir les prestations du GSU aux procédures de permis de construire, à la gestion des informations du contrôle des habitants (par ex. annonce de déménagement), aux écoles (accès pour les parents aux carnets scolaires, aux absences, etc.) ou encore au paiement des amendes en ligne. L'objectif du gouvernement cantonal est, à terme, d'offrir une seule adresse (www.GuichetUnique.ch) pour toutes les transactions publiques dans notre canton. Une utopie ? Certainement pas ! Car c'est là aussi un des nombreux atouts d'Internet à condition de faire preuve d'innovation et de souplesse : permettre la dématérialisation et la transmission aux conditions souhaitées de toutes les données gérées aujourd'hui encore sous forme de documents papier.

Enfin, pour l'administration publique et les autorités politiques, Internet a aussi complètement modifié le rapport à l'information et aux médias. L'Etat de Neuchâtel, qui vient de refondre complètement son site Internet, est appelé à communiquer toujours plus et toujours plus rapidement, pour tous les secteurs de l'administration, comme tout fournisseur de prestations. Le Conseil d'Etat doit quant à lui ajuster en permanence sa communication pour rester dans le cadre institutionnel qui est le sien tout en répondant aux nombreuses sollicitations des médias et de la population. Cela l'amène, pour ne pas dire le contraint, à aborder quasiment chaque dossier qu'il traite sous l'angle de la communication et à gérer en permanence l'instantanéité de l'information. Et là aussi la frontière entre vie politique et vie privée est parfois bien ténue…

Durant cette journée, vous allez partager des réflexions sur les droits, les obligations ou les problématiques liés à Internet au travail. Les quelques élément évoqués en introduction de cette journée vous auront convaincus, je l'espère, que les autorités neuchâteloises ont compris l'importance et les atouts de cet extraordinaire vecteur de communication. Dans les limites de leurs moyens et de leurs ressources, elles en ont fait usage pour fournir à leurs employés un cadre de travail moderne, attractif et efficace. Elles se sont aussi clairement positionnées pour progressivement transformer l'administration neuchâteloise et la rendre un jour accessible via Internet 24 heures sur 24, 7 jours sur 7 quel que soit le lieu où l'on se trouve et la prestation que l'on sollicite.

Mais ce formidable outil qu'est le réseau des réseaux ne doit pas nous faire oublier que nous avons toutes et tous également le devoir de fixer le cadre technologique, juridique et éthique dans lequel nous souhaitons le faire évoluer, en particulier sur nos lieux de travail. Afin que nous l'utilisions de manière performante et intelligente sans perdre de vue les risques et les dangers qu'il comporte. En ce sens, le colloque de ce jour organisé par la Chambre du commerce et de l'industrie et l'Université de Neuchâtel est à saluer. Je tiens à les remercier pour leur initiative commune ainsi que d'y avoir associé le Conseil d'Etat.

Laurent Kurth
Président du Conseil d'Etat neuchâtelois

Table des matières

Première partie - Cadre général et principes

Internet au travail : un cadre international rudimentaire, des solutions nationales contrastées **1**

Bertil Cottier

Docteur en droit, professeur ordinaire de droit de la communication à la Faculté des sciences de la communication de l'Université de la Suisse italienne, professeur associé à la Faculté de droit de l'Université de Lausanne

Entre liberté et surveillance : un regard anthropologique **23**

Daniela Cerqui

Maître d'enseignement et de recherche à l'Université de Lausanne

Internet au travail : droits et obligations de l'employeur et du travailleur **33**

Jean-Philippe Dunand

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

La *googlelisation* des employés respecte-t-elle les principes de la protection des données ? **73**

Christian Flueckiger

Préposé à la protection des données et à la transparence des Cantons de Neuchâtel et Jura, avocat, docteur en droit

La surveillance électronique des employés **99**

Sylvain Métille

Avocat, docteur en droit, chargé de cours à l'Université de Lausanne

Deuxième partie - Questions choisies

Utilisation des réseaux sociaux par les travailleurs et les employeurs **133**

Carole Aubert

Avocate, DEA en droit, criminalité et sécurité des nouvelles technologies, Neuchâtel

Régine Delley

Avocate, Chambre neuchâteloise du commerce et de l'industrie, Neuchâtel

Bref aperçu des aspects légaux du BYOD (Bring Your Own Device) **165**

Sébastien Fanti

Avocat, Sion

Utilisation d'Internet et de l'intranet par les syndicats et les représentants élus des travailleurs **205**

Geneviève Ordolli

Docteure en droit, Juriste au Service d'Assistance Juridique et Conseils (SAJEC) de la Fédération des Entreprises Romandes (FER), Genève

La réalisation d'un site web ou l'ouverture d'un compte par le travailleur. Qui est titulaire des droits ? **227**

Vincent Salvadé

Directeur général adjoint SUISA, professeur associé à l'Université de Neuchâtel

Nathalie Tissot

Docteure en droit, avocate, professeure à l'Université de Neuchâtel

Du papier à l'électronique : quels changements ? **255**

Olivier Subilia

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

Table des abréviations

ad	à
al.	alinéa(s)
ANSSI	Agence nationale de la sécurité des systèmes d'information (France)
APA	American Psychological Association
art.	article(s)
ATAF	Arrêt du Tribunal administratif fédéral
ATF	Recueil officiel des arrêts du Tribunal fédéral
BAG	Bundesarbeitsgericht (Allemagne)
BetrVG	Betriebsverfassungsgesetz (Allemagne)
BIT	Bureau International du Travail
BOCN	Bulletin officiel du Conseil national
BYOD	Bring Your Own Device
c.	contre
CC	Code civil suisse du 10 décembre 1907, RS 210
CCT	Convention collective de travail
CE	Communauté européenne
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 de l'Université de Lausanne
CEO	Chief executive officer
CF	Conseil fédéral
cf.	confer
ch.	chiffre(s)
CIA	Central Intelligence Agency
CMS	Content Management System
CNIL	Commission nationale de l'informatique et des libertés (France)
CO	Loi fédérale complétant le Code civil suisse du 30 mars 1911 (Code des obligations), RS 220
consid.	considérant (s)
contra	d'un avis contraire
CP	Code pénal suisse du 21 décembre 1937, RS 311.0
CPC	Code de procédure civile du 19 décembre 2008, RS 272
CPP	Code de procédure pénale suisse du 5 octobre 2007, RS 312.0
Cst.	Constitution fédérale de la Confédération suisse du 18 avril 1999, RS 101
CT	Code du travail du 2 janvier 1973 (France)

DTA	Revue de droit du travail et d'assurance-chômage, Zurich
éd.	édition
édit.	éditeur(s)
etc.	et cetera
FF	Feuille fédérale
GPS	Global Positioning System
ibidem	renvoie à la note précédente
IGF	Internet Governance Forum
in fine	à la fin
infra	plus bas
JAAC	Jurisprudence des autorités administratives de la Confédération, Berne
JAR	Jahrbuch des Schweizerischen Arbeitsrechts, Berne
JdT	Journal des Tribunaux, Lausanne
LAA	Loi fédérale sur l'assurance-accidents du 20 mars 1981, RS 832.20
LB	Loi fédérale sur les banques et les caisses d'épargne du 8 novembre 1934 (Loi sur les banques), RS 952.0
LBI	Loi fédérale sur les brevets d'invention du 25 juin 1954 (Loi sur les brevets), RS 232.14
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 du 9 octobre 1992 (Loi sur le droit d'auteur), RS 231.1
LEg	Loi fédérale sur l'égalité entre femmes et hommes du 24 mars 1995 (Loi sur l'égalité), RS 151.1
let.	lettre(s)
LOGA	Loi sur l'organisation du gouvernement et de l'administration du 21 mars 1997, RS 172.010
Loi sur la participation	Loi fédérale sur l'information et la consultation des travailleurs dans les entreprises du 17 décembre 1993, RS 822.14
LPD	Loi fédérale sur la protection des données du 19 juin 1992, RS 235.1
LPers	Loi sur le personnel de la Confédération du 24 mars 2000, RS 172.220.1
LPOV	Loi fédérale sur la protection des obtentions végétales du 20 mars 1975, RS 232.16
LPP	Loi fédérale sur la prévoyance professionnelle vieillesse, survivants et invalidité du 25 juin 1982, RS 831.40
LSCPT	Loi fédérale sur la surveillance de la correspondance par poste et télécommunication du 6 octobre 2000, RS 780.1
LTF	Loi sur le Tribunal fédéral du 17 juin 2005, RS 173.110
LTr	Loi fédérale sur le travail dans l'industrie, l'artisanat et le commerce du 13 mars 1964 (Loi sur le travail), RS 822.11

N	note(s) marginale(s)
n°	numéro(s)
NSA	National Security Agency
OCEl-PCPP	Ordonnance sur la communication électronique dans le cadre de procédures civiles et pénales et de procédures en matière de poursuite pour dettes et de faillite du 18 juin 2010, RS 272.1
ODAu	Ordonnance sur le droit d'auteur et les droits voisins du 26 avril 1993 (Ordonnance sur le droit d'auteur), RS 231.11
OFCOM	Office fédéral de la communication
OFJ	Office fédéral de la justice
OIT	Organisation Internationale du Travail
OJ	Loi fédérale d'organisation judiciaire du 16 décembre 1943 (abrogée)
Olico	Ordonnance concernant la tenue et la conservation des livres de comptes du 24 avril 2002, RS 221.431
OLPD	Ordonnance relative à la loi fédérale sur la protection des données du 14 juin 1993, RS 235.11
OLT 1	Ordonnance 1 du 10 mai 2000 relative à la loi sur le travail, RS 822.111
OLT 3	Ordonnance 3 du 18 août 1993 relative à la loi sur le travail (Hygiène), RS 822.113
OR	= CO
p.	page(s)
PFPDT	Préposé fédéral à la protection des données et à la transparence
PJA	Pratique juridique actuelle, Lachen
PME	Petites et moyennes entreprises
RCETF	Règlement du Tribunal fédéral sur la communication électronique avec les parties et les autorités précédentes du 5 décembre 2006, RS 173.110.29
réf.	référence(s)
rés.	résumé
RFJ	Revue fribourgeoise de jurisprudence, Fribourg
RJJ	Revue jurassienne de jurisprudence, Delémont
RO	Recueil officiel des lois fédérales
RS	Recueil systématique des lois fédérales (ou cantonales)
RSJ	Revue suisse de jurisprudence, Zurich
RSJB	Revue de la Société des juristes bernois, Berne
RSPI	Revue suisse de la propriété intellectuelle, Zurich
RVJ	Revue valaisanne de jurisprudence, Sion
s.	suivant
SA	société anonyme
SARB	Schweizerisches Arbeitsrecht, Bâle

SCSE	Loi fédérale sur les services de certifications dans le domaine de la signature électronique du 19 décembre 2003 (Loi sur la signature électronique), RS 943.03
SECO	Secrétariat d'Etat à l'économie
sic !	Revue du droit de la propriété intellectuelle, de l'information et de la concurrence, Zurich
SJ	La Semaine judiciaire, Genève
SMS	Short Message Service
SMSI	Sommet mondial sur la société de l'information
ss	suivants
SSA	Société suisse des auteurs
supra	plus haut
TF	Tribunal fédéral
TIC	Technologies de l'information et de la communication
UE	Union européenne
vol.	volume(s)
ZR	Blätter für Zürcherische Rechtsprechung, Zürich

Bibliographie générale

Cette bibliographie générale contient une liste des ouvrages et contributions les plus souvent cités dans ce livre. Elle est complétée par les bibliographies spécifiques qui se trouvent à la fin de chaque article.

BARRELET DENIS/EGLOFF WILLI, Le nouveau droit d'auteur, Commentaire de la loi fédérale sur le droit d'auteur et les droits voisins, 3e éd., Berne 2008.

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

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

DUNAND JEAN-PHILIPPE/MAHON PASCAL (édit.), Commentaire du contrat de travail, Berne 2013.

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

HOLENSTEIN CHRISTOPH, Die Benutzung von elektronischen Kommunikationsmitteln (Internet und Intranet) im Arbeitsverhältnis, Berne 2002.

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

ORDOLLI GENEVIÈVE, Intranet et internet dans les rapports collectifs de travail – Etude de droit suisse et de droit comparé, Genève 2013.

PERRIN JULIEN (édit.), Internet au lieu de travail, Lausanne 2004.

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.

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

STREIFF ULLIN/VON KAENEL ADRIAN/RUDOLPH ROGER, Arbeitsvertrag, Praxiskommentar zu Art. 319-362 OR, 7e éd., Zurich 2012.

SUBILIA OLIVIER/DUC JEAN-LUC, Droit du travail – Eléments de droit suisse, 2e éd., Lausanne 2010.

WYLER RÉMY, Droit du travail, 2e éd., Berne 2008.

WYLER RÉMY (édit.), Panorama II en droit du travail – Recueil d'études réalisées par des praticiens, Berne 2012.

Première partie

Cadre général et principes

BERTIL COTTIER*

Internet au travail : un cadre international rudimentaire, des solutions nationales contrastées

Sommaire Page

I. Internet au travail : un cadre international rudimentaire, des solutions nationales contrastées 2
A. Introduction 2
B. Le silence des instances internationales 3
1. L'absence de texte topique contraignant 3
2. Les raisons de ce silence 4
3. Les instruments cadre sur la protection des données 5
4. Et la *soft law* internationale ? 7
5. La jurisprudence de la Cour européenne des droits de l'homme 9
C. Les réponses nationales 11
1. Les lois sur la protection des données 11
2. La loi finlandaise sur le traitement des données personnelles de l'employé 13
D. Un bouquet de jurisprudences européennes hétéroclites 14
1. Généralités 14
2. L'arrêt *Nikon* (France) et ses suites 16
3. L'arrêt *Griffith c. Rose* (Australie) 17
E. Les USA légifèrent : les *Social media password protection Acts* 18
F. Conclusion 19

II. Bibliographie 20

* Je remercie Me Marcello Baggi, avocat à Lugano et collaborateur scientifique à l'Université de la Suisse italienne, pour son aide dans la rédaction cette contribution.

I. Internet au travail : un cadre international rudimentaire, des solutions nationales contrastées

A. Introduction

Du courrier électronique à la géolicalisation en passant par la vidéo-surveillance et les réseaux sociaux, les nouvelles technologies de la communication ont sans conteste impacté considérablement le monde du travail ces dernières décennies. Pour le meilleur ou pour le pire ? La réponse est sujette à controverses, les études réalisées n'apportant pas de conclusions unanimes[1]. Cela dit, que l'on soit un utilisateur enthousiaste de l'Internet ou l'un de ses plus véhéments détracteurs, force est de constater que ce vecteur de communication, s'il a grandement contribué à faciliter l'exécution des tâches assignées (que l'on songe à la popularisation du télétravail !), a aussi permis à l'employeur d'exercer une surveillance plus intrusive sur l'activité déployée par ses employés, que ce soit au poste de travail, en déplacement ou même à domicile. Surveillance sur le trafic d'ordre privé pour confondre qui vole du temps de travail en surfant abusivement sur la toile ou qui commet des infractions préjudiciables à l'entreprise (délits d'initiés, révélation de secret d'affaires ou encore espionnage économique). Surveillance aussi pour défendre la réputation de l'entreprise, avec pour cible première les employés déloyaux qui critiquent, contestent, vilipendent ou raillent leurs supérieurs (voire leurs collègues) sur *Facebook* ou *Twitter,* ou qui, depuis leur ordinateur professionnel, fréquentent des sites pornographiques ou des casinos en ligne.

En Europe comme en Amérique du Nord, cette surveillance accrue, si légitime soit-elle, a été vivement dénoncée au nom du respect de la vie privée ; à témoin – exemple certes extrême – ce « droit à la déconnexion » revendiqué par certains auteurs français[2]. Reste que, ici et là, le parlement quelques fois, les tribunaux ou les autorités de protection des données plus souvent, sont intervenus pour mettre le holà ; ces réactions sont toutefois contrastées, la vie privée n'étant pas sauvegardée au même degré d'un pays de l'autre.

La présente contribution traitera des réponses les plus intéressantes apportées par les Etats qui entourent la Suisse ou qui connaissent un taux très élevé d'utilisation d'Internet au travail comme les pays nordiques ou, bien entendu, les Etats-Unis. Un pays qui, con-

---

1 Et pas toujours pour le pire : une étude réalisée récemment en France a révélé que plus de 85% des cadres des entreprises de l'Hexagone jugent l'apport des nouvelles technologies de la communication positif ; et ce, bien que ces mêmes cadres soient les plus critiques à l'égard de leurs effets sociaux ; cf. LA DOCUMENTATION FRANÇAISE, *L'impact des TIC sur les conditions de travail*, Rapport et Documents 2012/49, p. 92 s.

2 Pour plus de détails sur ce droit encore et toujours hypothétique, voir RAY/BOUCHET.

trairement à un cliché tenace qui veut que la *privacy* n'y soit qu'une coquille vide, a tout récemment pris des mesures originales pour calmer l'insatiable curiosité de certains employeurs ; nous y reviendrons lorsque nous analyserons les *Social media password protection Acts*[3].

Avant de faire le tour de ces solutions nationales, une présentation du cadre international topique s'impose. Elle ne sera pas longue, car le droit supérieur contraignant, qu'il soit régional ou global, se révèle aussi fragmentaire que rudimentaire ; ce qui explique la vaste marge de manœuvre dont bénéficient, en la matière, les Etats souverains et, en conséquence, la diversité des règles qu'ils ont consacrées.

B. Le silence des instances internationales

1. L'absence de texte topique contraignant

Qui cherche une convention internationale traitant spécifiquement, en tout ou partie, de la surveillance des activités des employés sur Internet sera déçu. Bien que la problématique soit aussi actuelle que planétaire (la globalité du réseau des réseaux n'est plus à démontrer), les organisations internationales se sont abstenues, jusqu'à maintenant, d'aborder de front la question du monitorage excessif des employés. Qu'il s'agisse d'entités soucieuses des droits humains, et partant de la vie privée, comme le Conseil de l'Europe, ou d'entités qui ont pour vocation d'unifier, ou à tout le moins d'harmoniser le cadre juridique de la vie économique, au premier chef l'Union européenne (UE), ou encore d'entités spécialisées à l'instar de l'Organisation internationale du travail (OIT) ou de l'Internet Governance Forum (IGF), toutes répondent aux abonnés absents[4]. Aucun texte topique n'a été édicté ou n'est même en préparation.

On regrettera en particulier que l'OIT, qui se bat depuis bientôt plus d'un siècle pour améliorer les conditions de travail, semble négliger la question de la surveillance intrusive : pas même sa *Convention (187/2006) sur le cadre promotionnel pour la sécurité et la santé au travail*, un texte pourtant adopté à un moment où Internet était devenu l'apanage de tout un chacun, ne fait état des risques posés par un monitorage permanent

---

3 Cf. *infra* E.

4 Il est curieux que l'IGF, une émanation des Nations Unies et de l'Union internationale des télécommunications, créée pour installer, à l'échelon mondial, un dialogue sur les enjeux de l'Internet entre les parties prenantes (autorités public, société civile, milieux économiques, entreprises leaders sur le marché) n'a, à ce jour, jamais encore discuté du monitorage des employés. Et elle ne semble pas prête de le faire : la réunion annuelle de 2013, qui a rassemblé des milliers d'experts du monde entier à Bali, a abordé plus d'une centaine de sujets différents ; certains touchaient certes à la vie privée, mais aucun d'eux ne concernait notre sujet.

ou clandestin[5]. Pourtant la menace avait été clairement et précisément identifiée une dizaine d'années auparavant ; édicté en 1997 par le Bureau International du Travail (BIT[6]), le *Recueil de directives pratiques sur la protection des données personnelles des travailleurs* avait déjà posé quelques jalons pour prévenir les abus : d'une part une surveillance permanente ne saurait être autorisée que pour des raisons de sécurité et de santé ou en vue de protéger les biens de l'entreprise, d'autre part les travailleurs concernés devraient être informés à l'avance de la durée de la surveillance, des raisons qui la motive et de ses modalités d'exercice (en particulier de la technologie utilisée)[7].

2. Les raisons de ce silence

Pourquoi ce silence du législateur international ? Deux raisons peuvent être avancées.

D'abord la difficulté de trouver un consensus au sein de la communauté internationale pour réglementer le monitorage des employés, tant les approches politiques et juridiques divergent d'un Etat à l'autre. Au fossé, bien connu en droit comparé du travail, qui séparent les Anglo-Saxons, qui tendent à privilégier les intérêts de l'employeur, des Latins, encore très enclins à défendre avant tout les intérêts des travailleurs, s'ajoutent des visions diamétralement opposées sur la protection de la vie privée[8]. Certes la *privacy* a aujourd'hui rang de valeur universelle[9] ; reste que son respect est encore à géométrie

---

5 Significatif de ce « désintérêt », le magazine *Travail*, édité par l'OIT, n'a consacré qu'un seul article à la problématique de la surveillance ; et encore s'agissait-il d'une question pointue, l'usage abusif des puces d'identification par fréquence radio (*RFID et surveillance sur le lieu de travail*, 2007, p. 16 ss).

6 On rappellera que le BIT est le secrétariat permanent de l'Organisation internationale du Travail.

7 Voir le chiffre 6.14 de ces directives, lequel souligne en outre que « L'employeur doit réduire à un minimum l'ingérence dans la vie privée des travailleurs ». Le BIT a interprété cette disposition, à la lumière de l'évolution des nouvelles technologies, comme suit : « La multiplication de l'usage des ordinateurs et d'Internet au travail soulève de nouveaux risques et responsabilités tant pour les employeurs que pour les travailleurs. Tandis que les entreprises doivent prendre des mesures afin d'éviter l'accès non autorisé aux données confidentielles (y compris les données personnelles des employés), l'une des principales menaces auxquelles les travailleurs et leurs syndicats doivent faire face est la relative facilité avec laquelle les TIC peuvent envahir la vie privée des travailleurs à travers le contrôle de l'usage des appareils électroniques (par exemple, la lecture des courriers électroniques, le contrôle de la durée des appels téléphoniques) ou le contrôle des travailleurs eux-mêmes (par exemple, au moyen de caméras à circuits fermés) tant sur le lieu de travail que dans le contexte du télétravail. L'une des principales craintes est l'éventualité d'une vigilance continue ou dissimulée utilisée comme méthode d'intimidation ou de harcèlement sexuel. » (BIT, *ABC des droits des travailleuses et de l'égalité entre hommes et femmes,* 2008, p. 112).

8 Pour un aperçu de ces divergences, voir COTTIER, 2007, p. 80 ss.

9 Voir notamment l'art. 17 al. 1 du Pacte international relatif aux droits civils et politiques (RS 0.103.2) : « Nul ne sera l'objet d'immixtions arbitraires ou illégales dans sa vie privée, sa fa-

(très) variable, différences culturelles obligent[10]. Emblématiques à cet égard sont les relations orageuses entre l'Union européenne et les Etats-Unis en matière de protection des données : Bruxelles insiste pour imposer sa réglementation stricte aux entreprises américaines opérant en Europe alors que Washington s'acharne à les faire bénéficier du régime libéral qui prévaut outre-Atlantique[11].

Ensuite, on doit déplorer, partout, le profond embarras des législateurs nationaux face à une révolution de la communication dont, faute de connaissances techniques, ils ne perçoivent pas tous les tenants et aboutissants. Qui plus est, ils craignent que des normes spécifiques, visant des technologies concrètes, ne soient vite dépassées par un progrès scientifique fulgurant. Un embarras paralysant dont la conséquence peut se résumer en deux mots : *wait and see*. Si les législateurs nationaux sont à la peine, il en va de même, a fortiori, du législateur international, lequel dépend de l'existence de modèles nationaux pour son inspiration.

3. Les instruments cadre sur la protection des données

Cette passivité est confortée par le fait que, somme toute, une parade existe déjà au niveau international ; ce sont les textes qui régissent la protection des données. La surveillance des employés n'est en effet rien d'autre qu'un « traitement » de données personnelles régit par ces deux instruments fondateurs que sont la *Convention du Conseil de l'Europe de 1981 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel* (convention 108)[12] et la *Directive européenne 95/46 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel*[13].

---

mille, son domicile ou sa correspondance, ni d'atteintes illégales à son honneur et à sa réputation ».

10 Pour une brève mais pertinente présentation générale du concept de vie privée, voir POULET, p. 34.

11 Voir par exemple l'intéressante comparaison de la notion de vie privée aux Etats-Unis, au Sénégal et en Irlande faite par BRIERLEY NEWELL, p. 357 ss.

12 Pour un exposé des raisons qui ont créé ces divergences, voir HOAG, p. 811 ss ; ainsi que BENNETT, p. 161 ss. Pour un cas pratique, voir MALET, p. 1 ss.

13 RS 0.235.1.

Pour être complet, on mentionnera encore un texte plus particulier, mais sans impact direct sur notre domaine d'intérêt, la directive 97/66/CE concernant le traitement des données à caractère personnel dans le secteur des télécommunications. On signalera en outre que la directive 95/46 fait l'objet d'une refonte totale ; un nouveau texte plus contraignant (on parle d'un règlement, et non plus d'une directive) et aussi innovateur (consécration d'un droit à l'oubli, protection adaptée aux réseaux sociaux) pourrait prochainement entrer en vigueur. Quoi qu'il en soit, on restera au niveau d'une législation cadre posant des principes généraux en matière de protection des données ; il n'est pas question d'insérer des règles particulières en matière de surveillance en ligne de l'employé. Il est vrai que le projet de règlement mentionne la vidéo-surveillance à son art. 33 al. 2 ; cette disposition n'entend

Ce n'est pas le lieu de s'attarder sur ces instruments ; tout au plus rappellera-t-on qu'ils posent des préceptes généraux visant toutes les opérations, quelles qu'elles soient, portant sur des données personnelles. En bref, les traitements doivent respecter le principe de bonne foi (qui, notamment, s'oppose à la collecte clandestine de données), celui de proportionnalité (qui exige de choisir à chaque fois le traitement le moins intrusif possible) et celui de finalité (qui interdit la réutilisation des données pour un objectif non prévu à l'origine) ; de plus, la personne concernée se voit accorder un droit d'accès à ses données personnelles et un droit de blocage qui permet de s'opposer, sous certaines conditions, à un traitement ; enfin, des autorités de contrôle indépendantes doivent être créées[14]. On ne le répétera cependant jamais assez : tant la convention que la directive demeurent des textes cadre, truffés de concepts juridiques indéterminés et de vagues principes, dont la portée pratique dépend grandement des rapports de force en présence.

Cela dit, le « Groupe 29 », qui réunit les représentants des diverses autorités nationales de protection des données des pays membres de l'UE, a apporté des clarifications bienvenues (même si elles n'ont de valeur qu'indicative), dans son avis 8/2001 sur le traitement des données à caractère personnel dans le contexte professionnel et surtout dans son document de travail du 29 mai 2002 concernant la surveillance des communications électroniques sur le lieu de travail. Ce dernier texte, relativement circonstancié (près d'une trentaine de pages), se concentre avant tout sur l'information à donner aux employés en prônant l'adoption d'une charte d'entreprise sur la surveillance, laquelle définira à quelles conditions les salariés peuvent utiliser les moyens de communication professionnels et les modalités de contrôles éventuels ; le « Groupe 29 » invite en outre l'employeur à se lancer dans la surveillance qu'avec retenue : « Même si elle est nécessaire, toute mesure de contrôle doit être proportionnée au risque encouru par l'employeur. Dans la plupart des cas, l'utilisation abusive de l'Internet peut être détectée sans devoir analyser le contenu des sites visités » (chiffre 5.2).

Ce même « Groupe 29 » a récemment émis un avis (13/2011) sur les services de géolocalisation des *smartphones* ; ce texte aborde aussi la problématique sous l'angle des relations de travail, soulignant que : « l'employeur doit toujours (…) éviter une surveillance continuelle et par exemple choisir un système qui envoie une alerte lorsqu'un travailleur traverse une frontière virtuelle définie au préalable. Un travailleur doit pouvoir éteindre tout appareil de surveillance en dehors des heures de travail et la manière de le faire doit lui être expliquée. Les dispositifs de surveillance des véhicules ne sont pas des dispositifs de surveillance du personnel. Leur fonction est de repérer ou de contrôler la position des

cependant pas réglementer spécifiquement la matière, mais simplement limiter l'utilisation des images obtenues ; pour plus de détails, voir SEIFERT, p. 650 ss.

14 Pour une présentation de la convention 108 et de la directive 95/46, voir MEIER, respectivement p. 85 ss et 97 ss.

véhicules dans lesquels ils sont installés. Les employeurs ne devraient pas les considérer comme des dispositifs leur permettant de repérer ou contrôler le comportement ou les allées et venues de chauffeurs ou autres membres du personnel, par exemple en envoyant des alertes en rapport avec la vitesse du véhicule ».

4. Et la *soft law* internationale ?

Le mutisme du législateur international, s'il peut, à la rigueur, se comprendre au niveau du droit contraignant, surprend au niveau de la *soft law*. Après tout quand on s'engage à rien, on peut se montrer innovant et prospectif.

Instrument flexible et incitateur, la *soft law* se prête en effet particulièrement bien à la fourniture de réponses rapides et temporaires à des problèmes précis. Si les recommandations, codes de conduite et autres *best practices* abondent au niveau national lorsqu'il s'agit de réguler Internet en général et la surveillance en ligne des travailleurs en particulier, comme on aura l'occasion de le voir par la suite[15], ils se font très rares au niveau international. Ainsi, l'OIT, qui a plus de deux cents recommandations spécifiques à son actif, n'a rien entrepris dans le domaine des nouvelles technologies ; au contraire : ses recommandations les plus récentes concernent des thématiques on ne peut plus familières comme la pêche (199/2007), le travail domestique (201/ 2011) ou encore la sécurité sociale (202/2012)…

Au demeurant, on le sait (cf. *supra* B.1), le BIT a édicté, quant à lui, des directives en matière de protection des données personnelles des travailleurs. C'était cependant il y a plus de quinze ans, au temps des premières caméras de vidéo-surveillance, volumineuses et donc repérables ; depuis, la surveillance s'est faite insidieuse et mobile, et surtout a investi de nouveaux champs de contrôle, à commencer par les réseaux sociaux. On aurait pu s'attendre à ce que lesdites directives soient révisées pour prendre en compte ces nouveaux risques ; il n'en a rien été.

Gardien des libertés fondamentales, le Conseil de l'Europe se mobilise aujourd'hui tant sur le terrain des nouveaux médias que sur celui de la surveillance. Parfait ! Sauf que dans le premier cas, sa préoccupation première est de discipliner la liberté d'expression sur les réseaux sociaux[16] ; dans le second, il s'agit de renforcer la vie privée des citoyens face aux velléités de monitorage tous azimuts de ceux qui sont chargés de lutter contre le

15 Cf. *infra* C.

16 Voir par exemple la Recommandation 2012/4 du Comité des Ministres sur la protection des droits de l'homme dans le cadre des services de réseaux sociaux (laquelle met cependant en garde l'usager d'un service social contre les risques de laisser des traces : « des tiers, *comme les employeurs*, les compagnies d'assurance, […] sont notamment susceptibles d'accéder aux données à caractère personnel publiées dans un profil »).

terrorisme ou la criminalité organisée[17]. Sur la surveillance des employés proprement dite, il ne s'est guère exprimé, mis à part une (très générale) recommandation (1989/2) du Conseil des Ministres sur la *Protection des données à caractère personnel utilisées à des fins d'emploi* et une résolution (1233) de l'Assemblée parlementaire sur *l'Impact des nouvelles technologies sur la législation du travail.* Adoptée en l'an 2000, cette résolution commence, elle aussi, à dater. Cela dit, elle a le mérite non seulement d'identifier une foultitude de problèmes liés au recours aux technologies d'alors[18], mais de mettre en exergue un principe clef, celui de l'information préalable : « [il est recommandé] aux Etats membres de réaliser les adaptations juridiques nécessaires, afin d'adopter […] dans leurs législation et réglementation un niveau élevé de protection du travailleur […] par le droit d'information préalable du salarié de l'existence ou de la mise en place de fichiers nominatifs ou de dispositifs de surveillance des employés, ou de contrôle de leur productivité » (chiffre 11.c)[19].

Cela dit, on se doit de relever que la recommandation 89/2 est en passe d'être modernisée. En juillet 2013, le Comité consultatif de la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel a élaboré un avant-projet de révision destiné à prendre en compte les nouvelles technologies de communication[20]. Ladite recommandation serait complétée par une seconde partie posant des règles concrètes visant spécifiquement certaines « formes particulières de traitement ». Outre le rappel de l'exigence d'une information préalable, régulière et complète de l'employé sur les mesures prises, l'avant-projet dispose que :

Vidéo-surveillance (et autres moyens de surveillance à distance) (chiffre 14) : interdiction d'une surveillance délibérée et systématique d'un groupe de travailleurs (ou d'un

17 Dernier texte à ce sujet : la Déclaration du 11 juin 2013 du Comité des Ministres sur les risques présentés par le suivi numérique et les autres technologies de surveillance pour les droits fondamentaux.

18 L'art. 8 cite en vrac « la vidéosurveillance ; vérification des courriers électroniques ou du contenu des boîtes vocales ; surveillance des conversations téléphoniques ; fichage du salarié et détermination de son profil professionnel, de sa personnalité, de ses potentialités et de son état de santé ; évaluation de l'activité réelle du salarié, de son emploi du temps, de ses déplacements, et de sa productivité, par le port du badge électronique, l'autocommutateur, l'analyse des communications téléphoniques et des traces informatiques, etc. ».

19 On relèvera aussi que la recommandation 89/2 prévoyait déjà cette nécessité d'information préalable ; son art. 3 al. 1 souligne que « les employeurs devraient informer ou consulter leurs employés ou les représentants de ceux-ci préalablement à l'introduction ou à la modification de systèmes automatisés pour la collecte et l'utilisation de données à caractère personnel concernant les employés ».

20 T-PD(2013)05Rev. Ce texte est disponible sur le site : http://www.coe.int/t/dghl/standardsetting/dataprotection/default_fr.asp (consulté le 1er novembre 2013).

travailleur isolé) à moins que la mesure ne soit « une conséquence indirecte d'une surveillance nécessaire aux fins de la production, de la sécurité ou de l'organisation du travail de l'établissement » ;

Contrôle des connexions sur Internet (chiffre 16) : ce contrôle est licite, mais en tant que dernier recours ; auparavant, des mesures de blocage d'accès à certains sites problématiques devraient être prises. Quant à la surveillance des messages électroniques professionnels des employés, elle « ne peut survenir qu'en conformité avec la législation et si cela est strictement nécessaire pour des raisons de sécurité, de fonctionnement de l'entreprise ou pour d'autres raisons légitimes, telles que pour contrôler les infractions à la propriété intellectuelle de l'employeur » ; cela dit, les envois privés de l'employé ne peuvent jamais faire l'objet d'une surveillance ;

Géolocalisation (chiffre 17) : cette technologie n'est pas en soi bannie, mais elle ne doit pas être utilisée à des seules fins de surveillance ; un contrôle indirect est possible, pour autant que la surveillance soit primairement nécessaire à des fins de sécurité.

L'avant-projet ne traite cependant pas de la surveillance des activités de l'employé sur les réseaux sociaux ; tout au plus est-il souligné à l'art. 10 (transparence du traitement) que l'employeur devra tenir l'employé au courant des diverses catégories de données qu'il traite sur son compte : « une description particulièrement claire et complète devrait être fournie concernant les catégories des données à caractère personnel qui peuvent être collectées au moyen de systèmes et technologies d'information et leur utilisation potentielle, y compris la surveillance indirecte ».

5. La jurisprudence de la Cour européenne des droits de l'homme

Fondés sur l'article 8 de la Convention européenne des droits de l'homme, qui protège la vie privée (CEDH)[21], trois *leading cases* méritent d'être signalés, car ils posent des jalons quant aux limites du droit de l'employeur de surveiller ses employés ; des jalons importants, mais pas suffisants, car à eux seuls ils ne permettent pas de prévenir tous les risques.

Le premier arrêt (*Niemitz*[22]*),* qui concernait des fouilles entreprises par la police allemande dans le bureau d'un avocat, a vu les juges de Strasbourg reconnaître, en 1992 déjà, que l'employé doit pouvoir bénéficier d'un espace de vie privée même au travail ;

---

21 Art. 8 al. 1 de la Convention de sauvegarde des droits de l'homme et des libertés fondamentales (RS 0.101) : « Toute personne a droit au respect de sa vie privée et familiale, de son domicile et de sa correspondance ».

22 Niemitz c./Allemagne, du 23 novembre 1992.

les juges ont en effet relevé avec clarté et détermination que : « le respect de la vie privée doit aussi englober, dans une certaine mesure, le droit pour l'individu de nouer et développer des relations avec ses semblables. Il paraît, en outre, n'y avoir aucune raison de principe de considérer cette manière de comprendre la notion de vie privée comme excluant les activités professionnelles ou commerciales : après tout, c'est dans leur travail que la majorité des gens ont beaucoup, voire le maximum d'occasions de resserrer leurs liens avec le monde extérieur »[23].

Cette décision a été confirmée en 1997 dans l'arrêt *Halford*[24], qui visait plus directement des écoutes téléphoniques ; la Cour a au surplus eu l'occasion de préciser que les appels téléphoniques émanant de locaux professionnels sont a priori compris dans les notions de « vie privée » et de « correspondance » au sens de l'article 8 al. 1 CEDH.

Dix ans plus tard, la jurisprudence *Halford* a été transposée à l'ère d'Internet par l'arrêt *Copland*[25], qui concernait une secrétaire britannique que son employeur avait entrepris de surveiller, pendant plusieurs mois, au motif qu'elle était suspectée d'avoir une liaison inappropriée avec le directeur d'une entreprise concurrente. Les juges ont été d'avis que l'usage de l'Internet et du courrier électronique était aussi protégé par le droit au respect de la vie privée, lorsque le travailleur n'avait pas été informé d'éventuels contrôles et pouvait dès lors légitimement supposer que ces instruments de communication pouvaient servir à des communications privées : « N'ayant pas été prévenue que ses appels risquaient d'être surveillés, la requérante en l'espèce pouvait raisonnablement croire au caractère privé des appels passés depuis son téléphone professionnel. Il en va de même pour ses messages électroniques et ses connexions à des sites Internet »[26].

On retiendra de ces trois décisions que si l'employeur n'a pas formellement banni l'utilisation des moyens de communication professionnels ni ne s'est réservé la possibilité de faire des contrôles, l'employé peut prétendre à une pleine protection de ses communications privées ; ce d'autant que, comme l'ont relevé avec réalisme les juges dans l'arrêt *Niemitz*[27] : « on ne peut pas toujours démêler ce qui relève du domaine professionnel de ce qui en sort ». Reste à savoir si, dans l'hypothèse où l'employeur a interdit l'usage des moyens de communication professionnels, il a tout loisir d'entreprendre quelque contrôle que ce soit au motif que toute communication est présumée professionnelle. La Cour n'a pas abordé directement cette hypothèse ; toutefois, vu qu'elle a considéré, et dans l'arrêt *Halford* et dans l'arrêt *Copland*, la tolérance – expresse ou tacite – de

23 *Ibidem*, ad 29.
24 Halford c./ Royaume-Uni, du 25 juin 1997, ad 44.
25 Copland c./ Royaume-Uni, du 3 avril 2007, ad 42.
26 *Ibidem*, ad 42.
27 Niemitz c./Allemagne, ad 29.

l'employeur sur l'usage privé des moyens de communication de professionnels comme un critère de restriction des possibilités de surveillance, on penchera pour la libre surveillance dans le cas contraire[28].

C. Les réponses nationales

1. Les lois sur la protection des données

La convention 108 et la directive 95/46 (cf. *supra* B.3) ont entraîné l'adoption dans tous les pays européens de lois sur la protection de données, lesquelles reprennent les prescriptions générales posées par le droit supérieur tout en les précisant quelque peu. Il n'en demeure pas moins que, dans leur grande majorité, ces textes ne dépassent pas le stade de simples législations cadre. A l'exception notoire de la loi italienne[29] qui contient une partie spéciale (art. 46 à 140), laquelle pose des réglementations spécifiques pour des branches d'activités où les risques d'intrusions graves sont élevés, tels la poursuite pénale, la défense nationale, la santé, la sécurité sociale, ou encore les services financiers ; la loi est en revanche quasi muette sur les relations de travail, à l'exception d'un bref renvoi à l'article 4 de la loi 300 du 20 mai 1970, qui interdit les installations de vidéo-surveillance (et de tout autre appareil de contrôle à distance) sauf motif de sécurité[30].

Tous les pays européens ont institué des autorités indépendantes de protection des données (ici des commissions, là des préposés, c'est selon) dont la tâche est double : promouvoir la protection des données dans les divers secteurs de la vie sociale et économique et veiller à l'application correcte des législations topiques dans des cas précis. A cette fin, quelques autorités ont été dotées non seulement de compétences de décision et de sanction, mais aussi de véritables pouvoirs réglementaires[31]. Cependant, seules les autorités italienne et islandaise ont usé de pareils pouvoirs pour décréter des mesures, que l'on qualifiera, dans les deux cas, de rigoureuses. Le *Garante per la protezione dei dati personali* a établi des règles sur l'usage de la poste électronique au travail en

---

28 *Contra* « Groupe 29 », document de travail cité sous B.3.

29 *Codice in materia di protezione dei dati personali* 196/2003. A cela s'ajoute : la Norvège qui a intégré des règles sur la vidéo-surveillance dans un chapitre particulier de sa loi sur la protection des données, la Slovénie qui en a fait de même pour le *data mining*, ou encore l'Allemagne et l'Autriche qui ont ajouté des dispositions sur la notification des failles de sécurité. Pour plus de détails, voir COTTIER, 2014, ad B.1.

30 *Codice* art. 114.

31 Pour une présentation générale des pouvoirs des différentes autorités nationales de protection des données, voir Agence européenne pour les droits fondamentaux, *Data Protection in the European Union : the role of National Data Protection Authorities*, Luxembourg 2010.

2007[32] ; ce document important étend l'interdiction des installations de surveillance à distance, mentionnée dans le paragraphe précédent, aux logiciels de lecture des emails des employés, de collecte des données du trafic Internet ou encore des captures d'écran à distance[33] ; une quelconque information préalable des employés est sans effet sur cette interdiction de principe. Le préposé à la protection des données islandais a quant à lui réglementé, en 2006, la surveillance électronique et la géolocalisation des employés[34] ; on relèvera, entre autres, que ce texte très restrictif n'autorise l'employeur à accéder au courrier électronique qu'en cas de menaces graves pour les installations techniques, notamment la sécurité du réseau de communication ; que pareille surveillance doit en outre être notifiée au préposé, qui peut ordonner sa cessation immédiate s'il l'estime injustifiée. Dans tous les cas, la surveillance clandestine est interdite, sauf autorisation judiciaire.

D'autres autorités nationales de protection des données sont également intervenues ; cela dit, leurs textes n'ont pas force de loi, car il ne s'agit que de recommandations ressortissant de la *soft law*. Un exemple parmi d'autres, les *Restrictions à l'usage des « keyloggers »* de la *Commission française Informatique et Liberté* (2013), qui prévoient que les « keyloggers », ces dispositifs permettant d'enregistrer toutes les actions effectuées par un employé sur son poste informatique, ne peuvent être utilisés dans le cadre d'une relation de travail qu'en cas « d'impératifs forts de sécurité, et d'une information spécifique des personnes concernées »[35].

On ne saurait déduire de l'absence (ou du peu) de réglementations, voire de recommandations sur la surveillance électronique des employés, un quelconque désintérêt ou indifférence des autorités nationales de protection des données. Au contraire, s'il est un thème

---

32 *Linee guida del Garante per posta elettronica e internet*, Journal officiel n° 58 du 10 mars 2007.

33 Plus précisément : (6) « non può ritenersi consentito il trattamento effettuato mediante sistemi *hardware* e *software* preordinati al controllo a distanza, grazie ai quali sia possibile ricostruire –a volte anche minuziosamente– l'attività di lavoratori. É il caso, ad esempio :• della lettura e della registrazione sistematica dei messaggi di posta elettronica ovvero dei relativi dati esteriori, al di là di quanto tecnicamente necessario per svolgere il servizio *email* ; • della riproduzione ed eventuale memorizzazione sistematica delle pagine *web* visualizzate dal lavoratore ; • della lettura e della registrazione dei caratteri inseriti tramite la tastiera o analogo dispositivo ; • dell'analisi occulta di computer portatili affidati in uso. Il controllo a distanza vietato dalla legge riguarda l'attività lavorativa in senso stretto e altre condotte personali poste in essere nel luogo di lavoro ».

34 *Reglur um rafræna vöktun og meðferð persónuupplýsinga sem verða til við rafræna vöktun,* 837/2006 (disponible en traduction anglaise, sur le site : http://www.personuvernd.is/ (consulté le 1er novembre 2013).

35 On relèvera aussi que quelques pays ont réglé la question de la surveillance en ligne par le biais de conventions collectives de travail, à l'exemple de la Belgique (Convention collective de travail no 81/2002 relative à la protection de la vie privée des travailleurs à l'égard du contrôle des données de communication électroniques en réseau).

qui les préoccupe, c'est bien celui-ci ; néanmoins, plutôt que d'établir des prescriptions, les commissions ou les préposés privilégient le plus souvent une approche éducative, multipliant les feuilles d'information, les guides de sensibilisation et autres dossiers de bonnes pratiques. Ainsi la CNIL, encore elle, a émis des fiches pratiques sur la géolocalisation des salariés, sur la vidéo-surveillance sur les lieux de travail et sur les outils informatiques de travail ; régulièrement, mises à jour (la dernière fois en janvier 2013), ces trois documents présentent en langage simple, clair et précis les enjeux de la surveillance et les droits des protagonistes[36]. D'autres autorités consacrent plusieurs pages de leur site Internet à présenter les différentes facettes de la problématique[37].

2. La loi finlandaise sur le traitement des données personnelles de l'employé

C'est, à ce jour, la seule loi formelle qui traite de la surveillance des employés[38]. Si l'aval du parlement est toujours un gage de plus grande légitimité, il peut en revanche laisser craindre que le produit final ne soit édulcoré par des compromis et ne s'avère pas aussi rigoureux que les textes provenant des autorités de protection des données, tel le règlement islandais que nous venons de voir (cf. *supra* C.1). Craintes confirmée dans le cas présent : adopté en 2004 (mais à peine retouché depuis), ce texte, qui complète la loi nationale sur la protection des données (sans se substituer à elle), aborde aussi d'autres problèmes liés à la vie privée des travailleurs, à commencer par les examens médicaux ainsi que les tests d'alcoolémie et d'addiction aux drogues ; en matière de surveillance électronique, la loi demeure lacunaire, ne traitant que de la vidéo-surveillance proprement dite et de l'accès de l'employeur au courrier électronique en cas d'absence de l'employé.

Vidéo-surveillance (art. 16 s.[39]) : tout en insistant sur le plus de transparence possible lors de la mise en œuvre de cette mesure, la loi n'interdit pas la surveillance clandestine. Cela dit, la surveillance ne doit pas avoir pour but premier le contrôle des travailleurs mais le respect des processus de production, la sécurité de l'entreprise ou la sauvegarde de l'intégrité corporelle des travailleurs (prévention des rixes notamment). La caméra ne

36 Ces documents sont disponibles sur le site de la CNIL, http://www.cnil.fr/les-themes/travail/ (consulté le 1er novembre 2013).

37 Voir par exemple les informations très complètes de l'Inspectorat pour la protection des données suédois sur son site, http://www.datainspektionen.se/lagar-och-regler/personuppgiftslagen/arbetslivet/#kontroll (consulté le 1er novembre 2013).

38 Lag om integritetsskydd i arbetslivet (759/2004) ; disponible en traduction anglaise sur le site http://www.finlex.fi/en/laki/kaannokset/2004/20040759 (consulté le 1er novembre 2013).

39 Voir aussi le commentaire détaillé de l'autorité finlandaise de protection des données, *Integritetsskydd i arbetslivet*, 2008, p. 13 s.

doit jamais être dirigée directement sur un travailleur déterminé ; en outre, certains locaux sensibles, comme les vestiaires ou les toilettes, ne peuvent faire l'objet d'une surveillance. Quant aux modalités plus précises de la surveillance, le législateur, dans la plus pure tradition nordique de consensualité, invite les parties à les régler par le biais de la négociation (convention collective ou charte d'entreprise).

Accès au courrier électronique (art. 18 ss[40]) : les dispositions sont de nature supplétive, n'étant applicables que dans l'hypothèse où cette question n'aurait pas déjà été réglée d'un commun accord entre les deux parties. Partant du présupposé que l'on ne peut interdire aux employés d'utiliser les moyens de communication électronique à titre privé, le législateur entend prévenir le risque d'accès malencontreux à des courriers de nature non professionnelle. L'employeur n'est ainsi autorisé à consulter le contenu des mails adressés aux employés qu'à certaines conditions précises :

- il doit d'abord offrir à l'employé des solutions alternatives destinées à préserver son courrier privé tel un « répondeur automatique » qui informe l'expéditeur de l'absence de l'employé ou la déviation du courrier vers un collègue de confiance ; l'employé est toutefois libre de refuser ces propositions ;
- dans ce cas, l'employeur doit essayer de déduire le caractère professionnel ou non de l'envoi grâce à l'identité de l'expéditeur du courrier (un fournisseur ou un client laisse accroire un courrier professionnel) ou grâce à une éventuelle mention « personnel » sur l'entête du mail ; s'il conclut pour une nature professionnelle, il doit encore tenter de requérir le consentement de l'employé ; s'il ne l'obtient pas (ou si l'employé est décédé ou inatteignable), il sera enfin autorisé à prendre connaissance du contenu de l'envoi ;
- la consultation du courrier a lieu par l'intermédiaire de l'administrateur du système, lequel dresse un rapport écrit qui sera communiqué à l'employé à son retour.

D. Un bouquet de jurisprudences européennes hétéroclites

1. Généralités

On l'aura constaté : les réglementations topiques traitant de la surveillance des employés sont rares ; on comprend, dès lors, que les réponses nécessaires ont été dans la plupart des pays apportées par la jurisprudence, au coup par coup. De cette casuistique résulte un tableau fragmentaire et peu cohérent de la réalité juridique ; ce dont on dispose, c'est en

40 *Ibidem*, p. 15 ss.

effet moins de réponses que d'éléments de réponses. En bref, l'insécurité juridique est grande.

Grande parce que, mis à part la France, où la Cour de cassation a eu l'occasion, à plusieurs reprises, de se prononcer dans des affaires mettant en jeu l'usage des nouvelles technologies de surveillance[41], on déplore dans la plupart des pays une cruelle absence d'arrêts de principe des plus hautes instances nationales[42]. On doit donc se contenter de jugements d'instances inférieures, dont la pertinence reste sujette à caution ; d'autant plus que ces arrêts sont souvent contradictoires. Conséquence : la création d'une vaste zone grise qui nourrit les conflits de doctrine entre les auteurs qui émanent du droit du travail (en général plus libéraux) et ceux de la protection des données (plus restrictifs), mais que déplorent les entrepreneurs, lesquels réclament avant tout de connaître leurs limites.

L'Allemagne est exemplaire de l'insécurité juridique qui règne : le silence du *Bundesgerichthof* sur les possibilités pour l'employeur qui a toléré un usage privé des outils de communication professionnels d'accéder aux emails des employés a créé l'incertitude sur une question pourtant cruciale[43] : certaines cours admettent un accès sous conditions (notamment consultation en la présence du délégué à la protection des données de l'entreprise ; respect des envois désignés comme personnels[44]), d'autres le refusent,

41 Notamment sur la vidéo-surveillance comme en témoigne cet arrêt de principe de la Cour de cassation du 2 février 2011 : l'employeur qui a installé des caméras de surveillance pour des raisons de sécurité, peut néanmoins utiliser les enregistrements réalisés pour établir une faute disciplinaire. Cette jurisprudence sur le contrôle indirect, très favorable à l'employeur, a toutefois été tempérée dans une affaire de géolocalisation du 2 novembre 2011 ; la Cour a alors sanctionné un employeur qui avait détourné un système de géolocalisation placé sur le véhicule d'un employé, lequel bénéficiait de toute latitude pour organiser son travail à condition de respecter l'obligation de travailler 35 heures par semaine. Placé à l'origine pour assurer le contrôle des conditions de travail (aux fins d'améliorer les processus de production et optimiser les visites), le système avait été utilisé en fait pour mesurer le temps de travail effectif de l'employé en déplacement. Aux yeux des juges, ce détournement n'est pas justifié lorsque le salarié dispose d'une pleine liberté dans l'organisation du travail.

42 Encore plus rares sont les jugements des cours constitutionnelles ; pour un exemple récent, cet arrêt de la Cour constitutionnelle espagnole du 8 octobre 2013, qui d'un côté confirme que l'employeur a pleine latitude de contrôle si l'usage des moyens de communication professionnels a été interdit, de l'autre, juge que l'interdiction n'a pas besoin d'avoir été expressément signifiée par l'employeur ; une interdiction posée par une convention collective sectorielle suffit.

43 L'autre alternative - celle de l'employeur qui a interdit l'utilisation privée des moyens de communication professionnels (auquel est assimilé celui qui ne s'est pas prononcé sur le sujet) - est en revanche clairement réglée : l'employeur est sans autre en droit de contrôler.

44 Voir notamment l'arrêt du Landesgericht de Berlin du 16 février 2011.

jugeant que l'employeur tolérant doit être considéré comme un fournisseur de services Internet et partant est soumis au secret absolu des télécommunications[45].

Autre exemple de cette regrettable insécurité : les jurisprudences contradictoires sur la nature privée ou publique de *Facebook*. Ici on considère que le réseau social relève de la sphère privée, et donc les propos vexatoires ou critiques à l'égard de l'employeur, assimilables à une conversation de salon, sont impropres à justifier un licenciement pour faute grave ; là, *Facebook* est vu comme un moyen de communication de masse, donc l'employé déloyal peut être mis à la porte[46]. Valses hésitations qui ont finalement conduit la Cour d'appel de Rouen à se prononcer pour la double nature du réseau : « il ne peut être affirmé de manière absolue que la jurisprudence actuelle nie à *Facebook* le caractère d'espace privé, alors que ce réseau peut constituer soit un espace privé, soit un espace public, en fonction des paramétrages effectués par son utilisateur » [47]. Ce faisant, elle a annulé le licenciement d'une caissière qui avait invectivé sa hiérarchie sur le mur de son profil, mur dont l'accès était limité à une poignée d'amis[48].

Plutôt que de procéder à un recensement, décousu et contrasté, de décisions d'instances inférieures, on consacrera les sections suivantes à la présentation de deux arrêts de principe qui sont emblématiques du fossé qui sépare encore l'Europe continentale du monde anglo-saxon s'agissant de la surveillance en ligne de l'employé : une décision de la Cour de cassation française, l'arrêt *Nikon*, et une décision de la plus haute cour australienne, l'arrêt *Griffith*.

2. L'arrêt *Nikon* (France) et ses suites

L'arrêt de la Cour de Cassation française dans l'affaire dite *Nikon*[49] est, encore et toujours plus de dix ans après qu'il ait été rendu, une des décisions les plus claires en matière d'accès au courrier électronique des employés. Dans le sillage de la jurisprudence *Niemitz* de la Cour européenne des droits de l'homme (cf. *supra* B.5), les juges ont souligné que « Le salarié a droit, même au temps et lieu de travail, au respect de l'intimité

45 Pour plus de détails, voir PANZER-HERMEIER, p. 48 ss.

46 Pour un sommaire état des lieux de la controverse, voir TAMUR.

47 Cour d'appel du Rouen, arrêt du 25 novembre 2011.

48 Dans nombre d'autres pays, les tribunaux tendent, pour la plupart, à confirmer le licenciement en considérant que les réseaux sociaux sont des espaces publics, à l'instar de cette décision de l'Arbeitsgericht Bochum du 29 mars 2012 : « Allerdings hat der Kläger die Äusserungen nicht im Rahmen eines Chats mit Freunden getätigt, so dass die Äusserungen nicht als vertrauliches Gespräch unter Freunden oder Kollegen gewertet werden konnte. Denn gerade in der heutigen Zeit findet eine Konversation unter Freunden oft nicht mehr im persönlichen Gespräch, sondern im Rahmen von sozialen Netzwerken stat ».

49 Cour de cassation, 2 octobre 2001.

de sa vie privée ; celle-ci implique en particulier le secret des correspondances ; l'employeur ne peut dès lors sans violation de cette liberté fondamentale prendre connaissance des messages personnels émis par le salarié et reçus par lui grâce à un outil informatique mis à sa disposition pour son travail et ceci même au cas où l'employeur aurait interdit une utilisation non professionnelle de l'ordinateur ». La Cour de cassation a ainsi mis un frein aux volontés d'investigation de l'employeur : les courriers que l'employé a identifié comme privés (soit par le biais d'une indication « personnel » dans l'entête de l'email, soit, comme dans le cas d'espèce, par leur conservation dans un fichier électronique désigné comme personnel).

En revanche, les courriers qui ne sont pas identifiés comme privés sont présumés professionnels, comme la Cour de cassation a été amenée à le préciser dans plusieurs décisions ultérieures[50]. Dès lors, l'employeur « peut en prendre librement connaissance et les copier, s'en servir dans le cadre d'une procédure de licenciement et les produire tout à fait légalement dans le cadre d'un contentieux »[51]. Précision subséquente : l'employé n'est pas en droit de crypter le contenu de son ordinateur professionnel pour en entraver la consultation par son employeur[52].

3. L'arrêt *Griffith c. Rose* (Australie)

Cette décision[53], qui aborde la question cruciale de la surveillance de l'usage privé des moyens de communication professionnels est d'autant plus intéressante qu'elle émane d'un pays anglo-saxon, l'Australie, qui a pourtant adopté une loi sur la protection des données qui correspond aux sévères standards européens[54]. Peu importe, semble-t-il, puisque le droit de l'employeur de surveiller le trafic Internet de l'employé est garanti même s'il a toléré un usage privé des moyens de communications professionnels.

Griffith, un employé de la fonction publique, avait visité à quelques reprises des sites pornographiques (licites) depuis son domicile par le biais de son ordinateur portable professionnel. Ces visites avaient été détectées lors d'un contrôle technique de routine auquel sont soumises toutes les installations informatiques de l'administration publique. Griffith fut licencié pour violation du code de conduite des employés du secteur public qui interdit la consultation de site pornographique. Il recourut contre cette sanction sévère pour un employé jusque-là exemplaire, en arguant que l'employeur avait utilisé un

50 Notamment Cour de cassation, 15 décembre 2010.
51 GUIZARD-COLLIN.
52 Cour de cassation, 18 octobre 2006.
53 Federal Court of Australia, 31 janvier 2011.
54 Elle a été officiellement reconnue comme adéquate, et par la Commission européenne, et par le Préposé fédéral à la protection des données.

logiciel de surveillance (de marque *Spector360*) qui enregistrait toutes les opérations passées depuis l'ordinateur contrôlé, sans égard à ce qui pouvait être privé ; et ce, en violation d'une autre disposition de ce même code de conduite qui prévoyait que les mesures de surveillance doivent respecter la vie privée des employés.

Faisant peu de cas de cette cautèle, sauf à regretter, en passant, que pareils enregistrements à grande échelle ne puissent, accidentellement, révéler des transactions bancaires confidentielles (!), la Cour suprême australienne débouta Griffith sec et sonnant : le juge rapporteur a souligné que l'employeur, par le biais du code de conduite, avait clairement défini ce qui était inadmissible et partant était en droit de tout mettre en oeuvre pour veiller à son respect : « *Unlike the circumstance where Spector360 gratuitously collects personal banking information or credit card details during periods of personal use (which may very well involve a breach of privacy) what it collected from Mr Griffiths was the very thing it was intended to collect, namely, evidence of breaches of the Code of Conduct. It was also the very thing the Department had warned Mr Griffiths that it was going to monitor his use to detect. In those circumstances, I conclude that the collection of this particular information was not unfair within the meaning of Principle 1(2). It is not unfair to warn a person that their computer use will be monitored in order to detect any accessing of pornography and then to do so.* »[55].

E. Les USA légifèrent : les *Social media password protection Acts*

Ce titre générique recouvre plus d'une dizaine de textes législatifs d'Etats fédérés[56], lesquels battent pour la première fois en brèche le pouvoir jusqu'alors quasi absolu de l'employeur de monitorer, même clandestinement[57], le comportement de l'employé sur Internet[58] ; pouvoir encore renforcé par le fait que communication sur les réseaux sociaux n'est juridiquement pas considérée comme privée[59]. L'objectif est très précis :

---

55 Pour une critique de cet arrêt, voir SVANTESSON, p. 184 ss.

56 Le législateur fédéral s'étant à ce jour abstenu de réglementer la vie privée de l'employé, cette matière est entièrement de la compétence des Etats fédérés.

57 Voir GORMAN, notamment la jurisprudence commentée, p. 227 ss.

58 Deux exceptions : le Connecticut (Gen. Stat.§ 31-48d) et le Delaware (Del. Code § 19-7-705) qui exigent que l'employeur informe l'employé avant de procéder à un contrôle de sa messagerie électronique. Pour plus d'information sur cette toute puissance de l'employeur, voir MA, p. 296 ss, et WEISS, p. 16 ss. Voir aussi CONFORTI, p. 465, qui relève qu'en définitive un employé est beaucoup mieux protégé contre les écoutes menées par l'administration publique que contre les agissements de son employeur.

59 Tel est l'avis de la grande majorité de la doctrine, cf. BEDI qui rappelle que « The basic premise has not changed. Dubbed the Third Party Doctrine, it states that a person loses Fourth Amendment pro-

mettre un terme aux pressions exercées par l'employeur sur l'employé tendant à lui permettre de prendre connaissance de ses activités sur les réseaux sociaux.

Le pionnier en la matière fut l'Etat du Maryland qui, en 2012, a décidé de limiter les possibilités de l'employeur de surveiller les communications privées de ses employés sur les réseaux sociaux[60]. Si celui-ci demeure libre de procéder à des investigations sur les profils généralement accessibles, il lui est en revanche fait défense de requérir de l'employé ses mots de passe pour accéder à ses comptes sur Facebook et Twitter (ou autres) ou même d'exiger le statut d'« ami ». Ainsi, les activités privées de l'employé sur les réseaux sociaux demeurent hors de portée de l'employeur. Le non-respect de l'interdiction entraîne des sanctions pénales (amende de quelques milliers de dollars).

A ce jour, douze parlements d'Etats fédérés ont emboîté le pas du Maryland (une quinzaine d'autres sont sur le point de faire de même dans les mois prochains)[61]. Et ce, bien que les *Password Acts* aient subi la vindicte des employeurs qui déplorent ne plus être en mesure de détecter à temps des activités illicites graves telles la violation de secrets commerciaux et l'espionnage économique. Du côté des employés, on regrette que seules les lois de l'Illinois, du Michigan et de Washington bannissent aussi le *shoulder-surfing*, autrement dit l'injonction faite, à l'improviste, à l'employé de se connecter à son profil pour que l'employeur puisse le contrôler[62].

F. Conclusion

Au terme de ce bref tour d'horizon, un constat s'impose : s'il y a bien une certitude, c'est que l'incertitude règne, au niveau international, comme au niveau national.

Les réglementations qui visent spécifiquement et concrètement la surveillance électronique de l'employé se comptent sur les doigts d'une main. Et encore : celles qui existent sont pour la plupart lacunaires et/ou privées de force contraignante, émanant le plus souvent d'autorités de protection des données nationales qui ne bénéficient pas de pou-

---

tection—i.e., does not have a reasonable expectation of privacy—to any communications that the person voluntary discloses to another » p. 2. Reste que la Cour suprême n'a pas encore été amenée à se prononcer sur ce point.

60 *User Name and Password Privacy Protection Act* 2012. Pour une présentation générale des législations existantes en la matière, voir GORDON/SPATARO/SIMMONS.

61 Arkansas, Californie, Colorado, Illinois, Nevada, New Jersey, Nouveau-Mexique (la loi ne s'applique qu'aux candidats à un emploi), Oregon, Utah, Vermont et Washington.

62 Pour plus de détails sur les différences entre ces diverses législations étatiques, voir GORDON/HWANG.

voirs réglementaires. Elles relèvent en effet de la *soft law ;* qui plus est, elles traduisent le point de vue quelques fois partisan de leurs auteurs.

Certes, des réponses ponctuelles ont été apportées par la Cour européenne des droits de l'homme dans ces trois *leading cases* que sont *Niemitz, Halfort* et *Copland*, ou par des instances nationales qui se fondent soit sur d'anciennes interdictions de contrôle permanent relevant du droit du travail, soit sur les principes généraux de la protection des données, plus rarement sur le secret des télécommunications. Reste que l'on doit déplorer l'absence d'arrêts de principe dans nombre de pays, à commencer par l'Allemagne. Au-delà de certains acquis comme l'interdiction de la surveillance électronique constante, l'obligation d'informer les employés des mesures de contrôle envisagées et la graduation des mesures de contrôle à la gravité des infractions suspectées, cette casuistique, fragmentaire et contradictoire, ne permet pas de dissiper les nombreux doutes qui subsistent ; notamment sur ces questions centrales que sont :

- le droit ou non de l'employeur d'interdire l'usage des moyens de communication ;
- l'étendue de la surveillance exercée par l'employeur qui a admis l'usage privé des moyens de communication professionnels ;
- le droit ou non des employés de critiquer leur employeur sur les réseaux sociaux.

Guère de doutes en revanche aux Etats-Unis, où le pouvoir de surveillance de l'employeur sur l'usage des moyens de communication professionnels est absolu ; mais demain, peut-être, la donne changera, car les voix critiques de cette vision dictatoriale se font de plus en plus entendre. Assurément, l'exemple de ces quelques Etats fédérés, qui ont remis en question la toute-puissance de l'employeur au moyen des *Social media password acts*, a lancé un nouveau débat. Il était temps, car on avait presque oublié que les Etats-Unis avaient donné naissance, voici plus d'un siècle, au *right to be left alone*[63].

II. Bibliographie

BEDI MONU, Facebook and Interpersonal Privacy : Why the Third Party Doctrine Should Not Apply, Boston College Law Review 2013, p. 1 ss.

BENNETT STEPHEN, The « Right to Be Forgotten » : Reconciling EU and US Perspectives, Berkeley Journal International Law 2012, p. 161 ss.

BOSSU BERNARD, La géolocalisation ne doit pas être détournée de sa finalité, Revue du droit du travail 2012, p. 156 ss.

63 Voir l'article innovateur consacré à la protection de la personnalité en *common law* par WARREN/ BRANDEIS.

BRIERLEY NEWELL PARICIA, A cross-cultural comparison of privacy definitions and functions : a system approach, Journal of Environmental Psychology 1998, p. 357 ss.

CONFORTI JUSTIN, Somebody's Watching Me : Workplace Privacy Interests, Technology Surveillance, And The Ninth Circuit's Misapplication Of The Ortega Test In Quon V. Arch Wireless, Seton Hall Circuit Review 2012, p. 462 ss.

COTTIER BERTIL, Un régime unique de protection des données pour une pluralité de systèmes politiques, judiciaires, économiques et culturels : utopie ou réalité ?, in : Informatique : servitude ou libertés ? Les colloques du Sénat, Paris 2007, p. 80 ss (cité : COTTIER, 2007).

COTTIER BERTIL, Quoi de neuf à l'étranger ? Essai de bilan de l'activité récente des législateurs européens et américains, in : ASTRID EPINEY, Instruments de mise en oeuvre du droit à l'autodétermination informationnelle, Fribourg 2014 (à paraître) (cité : COTTIER, 2014).

GORDON/HWANG, Making Sense of the Complex Patchwork Created by Nearly One Dozen New Social Media Password Protection Laws, Washington 2013.

GORDON/SPATARO/SIMMONS, Social Media Password Protection and Privacy - The Patchwork of State Laws and How It Affects Employers, rapport publié par Littler Workplace Policy Institute, Washington 2013.

GORMAN DANIEL, Looking out for Your Employees : Employers' Surreptitious Physical Surveillance of Employees and the Tort of Invasion of Privacy, Nebraska Law Review 2006, p. 213 ss.

GUIZARD-COLLIN ALICE, Courrier électronique et licenciement pour faute grave, Droit & Technologies, 9 février 2011.

HOAG CAROLIN, In the Middle : Creating a Middle Road Between, U.S. and EU Data Protection Policies, Journal of the National Association of Administrative Law Judiciary 2013, p. 811 ss.

MA FRANCES, Copland v. United Kingdom : What is Privacy and How Can Transnational Corporations Account for Differing Interpretations, Loyola of Los Angeles International and Comparative Law Review 2009, p. 291 ss.

MALET JEAN-BAPTISTE, Amazon : l'envers de l'écran, Le Monde diplomatique, novembre 2013, p. 1 ss.

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

PANZER-HEEMEIER ANDREA, Der Zugriff auf diensliche E-mails, Datenschutz und Datensicherheit 2012, p. 48 ss.

POULET YVES, Autour du concept de Privacy : éthique et droits de l'homme dans la société de l'information ?, Les Dossiers Européens 2008, p. 34.

RAY/BOUCHET, Vie professionnelle, vie personnelle et TIC, Droit social 2010, n° 1.

ROSIER/GILSON, La vie privée du travailleur face aux nouvelles technologies de communication et à l'influence des réseaux sociaux : L'employeur est-il l'ami du travailleur sur Facebook ?, in : GILSON et alia (édit.), La vie privée au travail, Bruxelles 2011, p. 59 ss.

SEIFERT BERNARD, Neue Regeln über die Videoüberwachung, Visuelle Kontrolle im Entwurf des EU-Datenschutz-Grundverordnung, Datenschutz und Datensicherheit 2013, p. 650 ss.

SVANTESSON DAN, On line workplace surveillance – the view from down under, International Data Privacy Law 2012, p. 179 ss.

TAMUR EBRU, Facebook : Entre vie privée et vie publique, la justice n'a pas tranché, Widoobiz, 4 octobre 2012.

WARREN/BRANDEIS, The Right to Privacy, Harvard Law Review 1890, p. 193.

WEISS MARIE-ANDRÉE, The Use of Social Media Sites Data By Business Organizations in Their Relationship with Employees, Journal of Internet Law 2011, p. 16 ss.

DANIELA CERQUI

Entre liberté et surveillance : un regard anthropologique

Sommaire

		Page
I.	Un regard anthropologique	23
II.	La transparence, entre communication et surveillance	25
	A. Une société de l'information	25
	B. Internet, la colonne vertébrale d'une société transparente	26
III.	Vers de nouvelles formes de surveillance ?	27
	A. Sociétés disciplinaires et panoptisme	27
	B. Sociétés de contrôle	28
IV.	La sphère privée, en voie de disparition ?	30
V.	Bibliographie	30

I. Un regard anthropologique

L'usage d'Internet au travail pose indéniablement des questions aux employeurs comme aux employés, et cela qu'il s'agisse des usages professionnels ou des usages privés. En ce qui concerne les usagers professionnels, les emplois du secteur tertiaire supposent de nos jours systématiquement l'usage d'un ordinateur relié au réseau des réseaux, comme il est parfois coutume de nommer Internet. Les actes professionnels effectués par l'employé laissent donc des traces dans le système et l'employeur pourrait être tenté de les suivre pour s'assurer que l'employé fait bien son travail. En ce qui concerne les seconds, que celles et ceux qui n'ont jamais été tentés de mettre à profit leurs heures de travail pour effectuer une petite recherche d'ordre privé jettent la pierre ! Là encore, les employeurs pourraient être tentés de suivre les traces afin de s'assurer que leurs employés font leur travail et seulement leur travail.

Les secteurs primaire et secondaire ne sont toutefois pas épargnés par ces problèmes, entre autres parce que les smartphones peuvent permettre à tout un chacun d'accéder à Internet sur son lieu de travail même si l'ordinateur n'est pas un outil de travail. Dans ce

cas, l'employeur ne pourra pas contrôler l'historique des activités effectuées par le biais du réseau professionnel, mais un certain nombre d'activités en ligne de ses employés lui seront néanmoins facilement accessibles, ne serait-ce que sur les réseaux sociaux. Internet a en outre déjà été la cause de licenciements non seulement liés à son usage abusif durant les heures de travail[64], mais aussi de manière plus large pour des activités en dehors du travail, qu'il s'agisse de propos trop critiques tenus sur les réseaux sociaux à propos de l'entreprise[65], ou de récits de vacances ayant eu lieu durant une période d'arrêt maladie[66]. Plus largement, le simple fait de s'être connectée à Facebook à un moment où elle avait annoncé ne pas pouvoir travailler à cause d'une migraine l'obligeant à rester chez elle dans l'obscurité a coûté son travail à une employée bâloise[67].

Dans tous ces cas, différentes questions se posent pour qui cherche à porter un regard analytique sur le problème. Toute une série d'entre elles portent sur la question de savoir *comment* faire en sorte que les choses se déroulent de manière acceptable pour tous les acteurs concernés. Il peut par exemple s'agir de questions éthiques, de questions juridiques ou encore de questions en lien avec la sociologie de l'usage, qui ont pour point commun de prendre la situation actuelle comme point de départ et de chercher à résoudre les problèmes qui se posent *en aval*. Mon questionnement anthropologique, pour sa part, se penche sur la question de savoir *pourquoi* une société devient ce qu'elle est. En d'autres termes, il s'agit pour moi de comprendre quelles valeurs situées *en amont* nous conduisent à la situation actuelle et à interroger le projet de société sous-jacent à nos pratiques quotidiennes. Internet au travail apparaît dans cette perspective comme un cas révélateur de la logique de notre société en réseaux.

64 Voir par exemple http://www.pcinpact.com/news/83969-un-salarie-licencie-pour-27-a-50-messages-quotidiens-sur-facebook.htm (consulté le 28 octobre 2013).

65 Sous l'intitulé *Facebook et licenciement : les statuts qui les ont les fait virer*, CÉLINE CHAUDEAU signe un article, mis en ligne le 13 septembre 2013, qui fait le point sur six jugements appelés à faire jurisprudence sur le sujet. Cinq d'entre eux portent sur des propos diffamatoires tenus sur Facebook envers les supérieurs hiérarchiques ou plus généralement l'entreprise. http://www.cadremploi.fr/ editorial/conseils/droit-du-travail/detail/article/facebook-les-statuts-qui-les-ont-fait-virer-ou-pas.html (consulté le 28 octobre 2013).

66 C'est le cas évoqué par le sixième jugement analysé par CÉLINE CHAUDEAU.

67 Voir http://archives-lepost.huffingtonpost.fr/article/2009/04/30/1516052_licenciee-pour-avoir-surfe-sur-facebook-durant-son-arret-maladie.html (consulté le 1er novembre 2013).

II. La transparence, entre communication et surveillance

A. Une société de l'information

À en croire les discours des politiciens qui nous gouvernent, nous serions entrés depuis une dizaine d'années dans une nouvelle ère, dans laquelle tous les problèmes rencontrés par les êtres humains sont susceptibles d'être résolus par la libre circulation de l'information. Notre actuelle « société de l'information », aussi dite « société du savoir » ou encore « société de la connaissance », renvoie dans bien des esprits à un idéal d'égalité rendu possible par la circulation de l'information. Elle est en tous les cas désormais devenue une sorte de slogan politique et économique en ce sens qu'elle représente dans la bouche de nombre de nos dirigeants, l'horizon à atteindre pour obtenir un niveau de vie et de développement optimal pour le plus grand nombre[68]. Qualifiée aussi de société post-industrielle, elle tend à renvoyer exclusivement à l'échange d'informations, considéré le plus souvent aussi bien comme synonyme de communication que de savoir. En cela, il semble que nous soyons encore largement tributaires des premières définitions qui en ont été données dans les années 1970. En effet, alors que d'autres auteurs avant lui avaient en quelque sorte décrit la même chose sans toutefois la nommer (voir Richta), Bell a été l'un des premiers à vraiment théoriser ce type de société et à lui donner un nom, en l'occurrence celui de « société post-industrielle ». Selon lui, elle se caractériserait par cinq aspects fondamentaux : le passage d'un système de production de biens matériels à celui d'une économie de services (principalement santé, enseignement, recherche et administration) ; la transformation des structures de l'emploi dans le sens d'une prédominance de professionnels et de techniciens hautement qualifiés ; l'aspect central d'un savoir théorique générateur d'innovation et de croissance économique ; l'émergence de nouvelles technologies de l'esprit ; et, enfin, une maîtrise toujours accrue des développements techniques et sociaux. En résumé, Bell nous décrit une société de type tertiaire dont la condition première d'existence consiste en la circulation de l'information à tous les niveaux, d'où le rôle central accordé aux nouvelles technologies de l'information et de la communication.

Le fait de promouvoir une telle société est considéré comme prioritaire, comme l'atteste le « Sommet mondial sur la société de l'information » (SMSI) dont un premier volet s'est tenu à Genève en 2003 et un deuxième à Tunis en 2005. Organisé par un Comité des Nations Unies placé sous la présidence de Kofi Annan, le sommet a été initialement

[68] Pour une analyse critique et argumentée des discours liés à l'émergence de cette société, voir BERTHOUD/ISCHY/SIMIONI qui ont effectués une enquête de terrain auprès de représentants des secteurs scientifique, politique et économique.

suggéré par l'Union Internationale des Télécommunications. Selon le site Internet consacré à ce sommet, « *the modern world is undergoing a fundamental transformation as the industrial society that marked the 20th century rapidly gives way to the information society of the 21st century. This dynamic process promises a fundamental change in all aspects of our lives, including knowledge dissemination, social interaction, economic and business practices, political engagement, media, education, health, leisure, and entertainment. We are indeed in the midst of a revolution, perhaps the greatest that humanity has ever experienced. To benefit the world community, the successful and continued growth of this dynamic requires global discussion and harmonization in appropriate areas* »[69]. A lui seul, ce paragraphe de présentation met en évidence les espoirs placés dans la « révolution » de l'information, censée radicalement modifier nos vies quotidiennes pour donner lieu à un nouveau type de société.

B. Internet, la colonne vertébrale d'une société transparente

La mise en œuvre de ce nouveau type de société repose sur une infrastructure technologique dont Internet est le noyau central, d'où les efforts déployés simultanément par différents gouvernements pour favoriser son développement. Au niveau européen, un document intitulé « eEurope 2005 : une société de l'information pour tous » a été produit en 2002 afin d'aller en ce sens. Il y est affirmé que l'élargissement de la bande passante « contribuera à améliorer et simplifier la vie de tous les Européens et modifier les interactions entre individus, non seulement au travail mais aussi dans le cercle amical et familial »[70]. Descolonges parle pour sa part d'une « croyance, celle qui attribue aux techniques le pouvoir d'améliorer les relations entre les humains »[71]. Son analyse se fonde sur deux cas : l'URSS du XXe siècle et son industrialisation et les sociétés occidentales du début du XXIe siècle, avec leur fascination pour l'Internet. Dans les deux, elle met en évidence la volonté de créer un « nous », une sorte de fratrie grâce aux vertus de la technique. Pour ce faire, une condition première : chacun doit impérativement avoir accès à l'information. La même idée est présente dans des rapports américains, qui vont même encore plus loin. Ainsi, dans un rapport de la National Science Foundation sponsorisé par le Département du Commerce, sont examinées les différentes manières d'augmenter les performances de l'humain en matière d'échange d'informations. Certains contributeurs vont jusqu'à suggérer de modifier l'humain afin de lui ajouter un sens. Ainsi, un auteur constate-t-il que « *in our own case, because of the information*

69 http://www.itu.int/wsis/about/about_WhatIsWsis.html (cette citation ne se trouve plus sur le site actuel du SMSI: http://www.itu.int/wsis/index.html) (consulté le 1er novembre 2013).

70 COMMISSION DES COMMUNAUTÉS EUROPÉENNES, p. 9.

71 DESCOLONGES, p. 235.

explosion our species has created, I suggest that the most valuable sixth sense for our species would be a sense that would allow us to quickly understand, in one big sensory gulp, vast quantities of written information »[72]. Dans un tel contexte, les craintes suscitées par le *digital divide* séparant ceux qui ont et ceux qui n'ont pas accès à l'information sont énormes. Compte tenu de l'équation réductrice qui veut que l'accès à la technique conduise inéluctablement à la maîtrise de l'information – qui elle-même est prétendument synonyme de savoir, de richesse ou de prospérité – ce problème d'inégalité est considéré comme un obstacle majeur au développement de la société de l'information. Or ce fossé numérique, aussi mentionné dans les objectifs du Millénaire pour le développement comme un problème à résoudre avant 2015, subsiste indéniablement. Il reste donc une priorité politique majeure, c'est pourquoi le SMSI a été prolongé de « Forums SMSI » qui se déroulent chaque année, le dernier en date ayant eu lieu à Genève en mai 2013.

Dans cette logique, la transparence et la libre circulation des informations que permet Internet sont vues exclusivement sous leur angle positif, celui de la communication, de l'échange et de la liberté. Certains auteurs (voir par exemple Lévy) vont jusqu'à affirmer que les technologies de l'information permettent la réalisation des idéaux de la Révolution française, soit liberté, égalité, fraternité.

III. Vers de nouvelles formes de surveillance ?

A. Sociétés disciplinaires et panoptisme

Or, qui dit transparence dit aussi contrôle et surveillance. Ces derniers ne sont en rien des effets collatéraux, mais bel et bien le revers de la médaille de la transparence. En d'autres termes, il est impossible d'avoir l'un sans l'autre. Les technologies de l'information directement appliquées à la surveillance, telles que les caméras ou les logiciels dits espions ne sont que la pointe d'un iceberg dans lequel toutes les technologies de communication contribuent, du moins potentiellement, à un contrôle des individus.

Dans son magnifique ouvrage intitulé *Surveiller et punir. Naissance de la prison*, Foucault analyse la mise en place de la société disciplinaire dès le XVIII^{e} siècle. La prison en est la figure emblématique, mais d'autres espaces d'enfermement, tels que les hôpitaux et les écoles font également partie du système qu'il décrit. Il s'agit d'un modèle dans lequel les corps font l'objet d'une discipline rigoureuse, pratiquement inspirée de la vie

72 SPOHRER, in : BAINBRIDGE/ROCO, p. 109.

monacale, visant une normalisation des comportements et donc un contrôle social. En ce sens, la discipline « est la technique spécifique d'un pouvoir qui se donne les individus à la fois pour objets et pour instruments de son exercice »[73], chacun exerçant une forme de contrôle sur chacun. Le panoptisme, inspiré de Jeremy Bentham, remplit un rôle fondamental dans ce processus. Tel que conceptualisé par Bentham, il s'agit d'un dispositif architectural construit de telle manière qu'un surveillant placé dans un dispositif central puisse surveiller tous les « détenus ». Foucault le décrit comme suit : « à la périphérie un bâtiment en anneau ; au centre une tour ; celle-ci est percée de larges fenêtres qui ouvrent sur la face intérieure de l'anneau ; le bâtiment périphérique est divisé en cellules, dont chacune traverse toute l'épaisseur du bâtiment ; elles ont deux fenêtres, l'une vers l'intérieur, correspondant aux fenêtres de la tour ; l'autre, donnant sur l'extérieur permet à la lumière de traverser la cellule de part en part. Il suffit alors de placer un surveillant dans la tour centrale, et dans chaque cellule d'enfermer un fou, un malade, un condamné, un ouvrier ou un écolier. Par l'effet du contre-jour, on peut saisir de la tour, se découpant exactement sur la lumière, les petites silhouettes captives dans les cellules de la périphérie. Autant de cages, autant de petits théâtres, où chaque acteur est seul, parfaitement individualisé et constamment visible »[74] ; la visibilité constituant un piège. Toujours à en croire Foucault, Bentham vise non seulement à créer une « institution disciplinaire parfaite »[75], mais aussi à montrer que la discipline peut, sans enfermement, se diffuser dans l'ensemble du corps social. Pour ce faire, il rêve de faire du panoptisme « un réseau de dispositifs qui seraient partout et toujours en éveil, parcourant la société sans lacune ni interruption »[76]. Vu sous cet angle, le réseau informatique constitue une parfaite réalisation du panoptisme.

B. Sociétés de contrôle

Deleuze a actualisé les concepts de Foucault en décrivant le passage d'une société disciplinaire où le pouvoir s'exerce en espace clos, à une société dans laquelle le contrôle s'exerce en milieu ouvert. Il évoque la crise des institutions d'enfermement et décrit un système dans lequel l'individu n'a plus rien d'indivisible, le contrôle s'exerçant désormais au niveau « dividuel ». En d'autres termes, ce n'est plus l'individu pris dans son ensemble qui est objet de surveillance, mais ce dernier est analysé et maîtrisé par le biais des différents paramètres qui le constituent. Deleuze insiste en particulier sur le rôle du marché dans ce processus, le marketing étant devenu selon lui le principal outil de con-

73 FOUCAULT, p. 172.
74 FOUCAULT, p. 201-202.
75 FOUCAULT, p. 210.
76 FOUCAULT, p. 210.

trôle de tout un chacun par sa stratégie de ciblage des comportements d'achat. Ainsi, « [l]es individus sont devenus des *dividuels* et les masses, des échantillons, des données, des marchés ou des *banques* »[77]. Force est de constater que le modèle décrit par Deleuze il y a plus de vingt ans s'est largement développé, comme en témoignent les nombreuses cartes de fidélité des magasins qui découpent et comptabilisent nos comportements d'achats. A cela sont venues s'ajouter les activités en ligne par le biais desquelles tout utilisateur laisse de nombreuses traces dont l'accumulation, mais aussi le recoupement, pourraient conduire à reconstituer l'ensemble de ses comportements. Les plateformes d'échanges rendues possibles par l'apparition du web 2, on pense en particulier à des réseaux sociaux tels que facebook, fournissent dès lors, sous couvert de communication, de formidables outils de contrôle, déjà largement dénoncés par des instances telles de que la Commission Informatique et Libertés (CNIL).

Si la société de contrôle décrite par Deleuze se diffuse donc peu à peu, la société disciplinaire analysée par Foucault n'en disparaît pas pour autant. On peut observer actuellement que les espaces d'enfermement sont loin d'avoir disparu. Mais leurs modalités de fonctionnement ont été redéfinies par l'apparition de possibilités de contrôle à distance permises par les technologies de l'information. Ainsi, les peines pénitentiaires se doivent de prendre en compte les possibilités offertes par les bracelets électroniques, de même que les soins en milieu hospitalier doivent être coordonnés avec les multiples possibilités de surveiller le patient en dehors de ce cadre. En d'autres termes, la société de contrôle n'a pas remplacé la société disciplinaire. Les modalités de contrôle qui lui sont propres sont venues se rajouter à celles qu'avait décrites Foucault ouvrant donc d'énormes possibilités de contrôle social.

En résumé, en ce qui concerne Internet, il est, comme je l'ai laissé entendre plus haut, une réalisation du rêve de Bentham, en permettant un panoptisme sans limites. Chaque utilisateur sait pertinemment que ses moindres gestes virtuels peuvent faire l'objet d'un monitoring, mais ne sait pas si c'est effectivement le cas, tout comme le prisonnier du bâtiment périphérique ne sait pas, à cause du contrejour, si le surveillant est en train de l'observer. Au phénomène du contrôle effectif exercé par autrui, il y a donc lieu d'ajouter l'auto-contrôle social engendré par le fait d'être potentiellement surveillé, à plus forte raison quand il est question du monde du travail.

En outre, Internet est aussi un espace dans lequel nous n'agissons pas dans notre entièreté. Selon que nous sommes actifs dans les réseaux sociaux, sur des sites de vente ou encore dans la recherche d'informations sur des thèmes particuliers, les traces que nous laissons donnent des éclairages partiels sur nos comportements. Mis ensemble à l'image

77 DELEUZE, p. 112, souligné par l'auteur.

des pièces d'un puzzle, ces différents paramètres permettent de reconstituer l'individu devenu dividuel.

En d'autres termes, les technologies de l'information, Internet en tête, sont le fruit d'une société qui allie la discipline de Foucault et le contrôle de Deleuze, ce qui ne peut pas ne pas avoir de conséquence, en particulier en ce qui concerne la question du respect de la sphère privée.

IV. La sphère privée, en voie de disparition ?

La liberté individuelle, censée trouver sa consécration dans une société connectée, s'accompagne théoriquement de la nécessité du respect de la sphère privée. Or, de par sa nature même, le réseau suppose qu'il n'y ait aucune entrave à la circulation de l'information, d'où les possibilités de contrôle qui en découlent. Ainsi, très paradoxalement, les technologies supposées permettre à notre liberté de s'exprimer sont aussi celles qui rendent possibles les intrusions dans notre sphère privée. Le vieil adage selon lequel la liberté des uns s'arrête là où commence celle des autres prend ici tout son sens ; ou plutôt devrait prendre tout son sens, mais ce n'est pas toujours le cas. En effet, l'idéologie liée à la nécessité d'accéder à l'information en temps réel et sans barrière d'aucune nature est tellement largement partagée que chacun d'entre nous veut pouvoir accéder à ce tout ce qu'il souhaite, mais aimerait en même temps voir sa propre sphère privée respectée. Or, si chacun demande le respect de sa propre sphère, alors toute la logique de circulation sans limites se trouve entravée. Il va en conséquence tôt ou tard falloir faire un choix entre ces deux valeurs aussi largement partagées que contradictoires, que sont la liberté d'accès et le respect de la sphère privée. La tendance actuelle donne à penser que c'est plutôt à la sphère privée que nous renoncerons, et le risque est donc grand de voir la société de surveillance, faite de discipline et de contrôle, se développer de plus en plus.

V. Bibliographie

BAINBRIDGE/ROCO (édit.), Societal Implications of Nanoscience and Nanotechnology, Arlington : National Science Foundation, 2002.

BELL DANIEL, Vers la société post-industrielle, Paris 1976.

BERTHOUD/ISCHY/SIMIONI, La société de l'information : la nouvelle frontière ?, Lausanne 2002.

COMMISSION DES COMMUNAUTÉS EUROPÉENNES, eEurope 2005 : une société de l'information pour tous, Communication de la Commission au Conseil, au Parlement européen, au Comité économique et social et au Comité des régions, Bruxelles 2002.

DELEUZE GILLES, Post-scriptum sur les sociétés de contrôle, L'Autre Journal, Mai 1990.
DESCOLONGES MICHÈLE, Vertiges technologiques, Paris 2002.
FOUCAULT MICHEL, Surveiller et punir, Naissance de la prison, Paris 1975.
LÉVY PIERRE, La cyberculture en question : critique de la critique, Revue du M.A.U.S.S, 1997.
RICHTA RADOVAN, La civilisation au carrefour, Paris 1969.

JEAN-PHILIPPE DUNAND*

Internet au travail : droits et obligations de l'employeur et du travailleur

Sommaire

Page

I. Introduction 34

II. Obligations et responsabilité du travailleur 36
A. Devoir de diligence et de fidélité (art. 321*a* CO) 36
B. Utilisation privée d'Internet 38
1. Notion 38
2. Utilisation privée autorisée ou interdite 39
3. Critères déterminants 41
a) Prestation de travail 41
b) Coûts financiers 42
c) Sécurité, confidentialité et réputation de l'entreprise 43
d) Contenu 44
C. Responsabilité du travailleur (art. 321*e* CO) 45
D. Licenciement avec effet immédiat (art. 337 CO) 46
1. Principes 47
2. Jurisprudence sur l'usage abusif des moyens informatiques 47
a) Licenciements immédiats injustifiés 47
b) Licenciement immédiats justifiés 48

III. Obligations et responsabilité de l'employeur 49
A. Devoir de protection de la personnalité : principes généraux 49
B. Disponibilité continue 50
C. Harcèlement 52
1. Harcèlement psychologique 53
2. Harcèlement sexuel 54
D. Protection des données 56
1. Levée du courrier électronique 56
2. Cybersurveillance 58
E. Responsabilité de l'employeur 61

---

* Cette contribution constitue une version complètement remaniée et adaptée d'un article intitulé « L'usage de l'Internet sur le lieu de travail au vu de la jurisprudence récente du Tribunal fédéral », paru in : Julien Perrin (édit.), Internet au lieu de travail, Lausanne 2004, 1-35. Je remercie Nicolas Brügger, avocat, assistant-doctorant, et Héloïse Rosello, assistante-doctorante, pour l'aide apportée à la recherche de documentation.

IV. Règlement d'utilisation 63
A. Communication du règlement 63
B. Droits et obligations des employés 64
C. Mesures de surveillance 66
D. Sanction des abus 67
E. Mesures techniques 69
V. Conclusion 70
VI. Bibliographie 71

I. Introduction

Les moyens informatiques constituent un instrument de travail incontournable dans les entreprises de notre pays. La plupart des employés qui travaillent en Suisse sont connectés à Internet par le biais d'un navigateur hypertexte et d'une ou plusieurs adresses de courriers électroniques[1]. On distinguera les activités qui nécessitent l'enregistrement de données (messagerie électronique, téléchargement de fichiers, etc.) de celles qui ne nécessitent pas l'enregistrement de contenu sur un support de données (navigation sur le web, forums de discussion, etc.). L'évolution de la technologie favorise l'interaction et permet désormais à tout utilisateur de devenir un créateur de contenu qu'il met à disposition des autres internautes (création de Blogs, envoi de Tweets, etc.)[2]. L'accès à Internet est très aisé. Il suffit le plus souvent à l'utilisateur de s'identifier et de frapper son mot de passe. La connexion s'effectue autant depuis un ordinateur fixe qu'au moyen d'un ordinateur portable, d'une tablette électronique, d'un smartphone ou même d'une imprimante en réseau.

L'informatique a permis dans de nombreux secteurs économiques d'augmenter l'interactivité, la productivité et la rentabilité. Elle rend les employés plus autonomes et performants[3]. L'accès à Internet et à la messagerie électronique est devenu incontournable pour communiquer à l'intérieur et à l'extérieur de l'entreprise, recruter des candidats, transmettre des documents, gérer les comptes bancaires, rechercher des informations, accéder à certaines formations internes à l'entreprise (par exemple, sur le serveur Intranet de l'entreprise), faire héberger des solutions informatiques par des tiers (par exemple, service de stockage distant, *cloud computing*) ou encore améliorer la visibilité

1 SUBILIA, p. 39.
2 EGLI, N 2.
3 PASCHE, p. 70.

et l'e-réputation[4]. Dans le même temps cependant, l'utilisation des moyens informatiques génère des risques importants, autant pour l'entreprise (par exemple, vol ou destruction de données, atteinte à la réputation) que pour les employés (par exemple, surveillance abusive, intrusion dans la sphère privée)[5].

Le développement fulgurant des moyens informatiques a contribué à transformer en profondeur les rapports de travail. Ces nouvelles technologies rendent moins certaines les notions de lieu et de temps de travail, et aussi, par conséquent, de lien de subordination[6]. Il est désormais possible d'accéder aux ressources du réseau de l'entreprise en se connectant sur Internet depuis n'importe quel lieu (au moyen, par exemple, des réseaux privés virtuels, Virtual Private Network, VPN). La prestation de travail peut dès lors s'effectuer dans un autre lieu que l'entreprise, par exemple au domicile du travailleur (travail à domicile, télétravail) ou dans différents endroits où se trouve le travailleur (« bureau satellite » ; « travail nomade »)[7]. Par ailleurs, l'horaire et le temps de travail deviennent eux aussi plus incertains, même pour les employés travaillant principalement dans l'entreprise, car il est assez fréquent d'effectuer des prestations de travail en dehors de l'horaire initialement convenu en utilisant les moyens technologiques à disposition (ordinateur, smartphone, etc.). Enfin, contrairement à la règle selon laquelle c'est l'employeur qui fournit au travailleur les instruments de travail (cf. art. 327 al. 1 CO), l'ordinateur ou le téléphone portable utilisés comme instruments de travail appartiennent parfois à l'employé (pratique appelée dans la terminologie anglaise BYOD, « Bring Your Own Device », soit « apportez vos propres terminaux »)[8].

L'usage d'Internet sur le lieu de travail pose de nombreuses questions juridiques qui sont loin d'être résolues. Les développements technologiques sont toujours plus rapides que le droit. En l'absence de réglementation spécifique, il faut recourir aux dispositions du Code des obligations sur le contrat de travail (art. 319 ss CO), ainsi qu'aux règles contenues dans la législation sur le travail et sur la protection des données. On tiendra également compte des règlements et directives qui ont été adoptés par de nombreuses entreprises et administrations publiques.

Nous traiterons dans cette contribution des obligations et de la responsabilité du travailleur (chapitre II) avant d'analyser les obligations et la responsabilité de l'employeur (chapitre III). Nous examinerons ensuite les modalités de la rédaction d'un règlement

4 LANGHEINRICH/KARJOTH, p. 50 ss ; PASCHE, p. 72 ss.
5 BAUMGARTNER, p. 1434 ss ; EGLI, N 20 ss ; PASCHE, p. 72.
6 DUNAND, L'usage de l'Internet, p. 9.
7 GEISER, Neue Arbeitsformen, p. 565.
8 Sur cette pratique et les nombreux problèmes juridiques qu'elle suscite, voir BIRKHÄUSER/HADORN, ainsi que la contribution de SÉBASTIEN FANTI dans le présent ouvrage, p. 165 ss.

d'utilisation et de surveillance des moyens informatiques (chapitre IV). La présentation se veut générale : de nombreux aspects sont approfondis dans les autres contributions de l'ouvrage.

II. Obligations et responsabilité du travailleur

Puisqu'il n'existe pas de dispositions topiques, les obligations et la responsabilité du travailleur qui utilise Internet dans ses relations de travail s'analysent en fonction des règles générales sur le contrat de travail. L'article 321*a* CO, qui régit le devoir de diligence et de fidélité, est particulièrement important (section A). L'utilisation d'Internet à des fins privées pose des questions délicates (section B). Le travailleur est susceptible d'engager sa responsabilité contractuelle, selon l'article 321*e* CO si, par l'utilisation d'Internet, il cause un dommage à son employeur (section C). Enfin, l'employé qui viole gravement ses devoirs court le risque d'être licencié avec effet immédiat, aux conditions prévues à l'article 337 CO (section D).

A. Devoir de diligence et de fidélité (art. 321*a* CO)

Le travailleur doit fournir sa prestation de travail de manière diligente et fidèle (art. 321*a* al. 1 CO). Selon son obligation de diligence, il est tenu d'exécuter « avec soin le travail qui lui est confié » (art. 321*a* al. 1 CO). Il observera à cet effet les directives générales de l'employeur sur l'exécution du travail, ainsi que les instructions particulières qui lui ont été données (cf. art. 321*d* al. 2 CO)[9]. Le devoir d'exécution diligente comprend celui de traiter « avec soin » le matériel mis à disposition par l'employeur, « selon les règles en la matière » (art. 321*a* al. 2 CO). Quant à l'obligation de fidélité, elle comporte un aspect positif et un aspect négatif : elle consiste à mettre toutes ses forces au service de l'employeur et à renoncer à tout ce qui pourrait lui nuire[10]. L'obligation de fidélité interdit aussi au travailleur d'utiliser ou de révéler « des faits destinés à rester confidentiels » (art. 321*a* al. 4 CO). Elle impose en outre au travailleur une obligation de rendre compte et de restituer, qui existe autant pendant les rapports de travail (cf. art. 321*b* CO), qu'au moment où le contrat prend fin (cf. art. 339*a* CO).

Lorsqu'il consacre une partie de son temps de travail à des activités récréatives, par exemple à jouer aux cartes sur son ordinateur, au détriment de ses tâches profession-

9 DUNAND, Commentaire, N 9 ad art. 321*a* CO, p. 56.
10 DUNAND, Commentaire, N 12 ad art. 321*a* CO, p. 56.

nelles, le travailleur adopte une attitude contraire à l'art. 321*a* al. 1 CO[11]. Plus généralement, l'employé s'abstiendra de toute activité qui contreviendrait à la loi ou aux instructions reçues, exposerait l'entreprise à des prétentions de tiers, ou risquerait de provoquer la paralysie de son réseau informatique[12].

L'employé renoncera, par exemple, à émettre sur les réseaux sociaux des critiques envers ses supérieurs hiérarchiques ou la stratégie de l'entreprise[13]. Peut constituer une violation du devoir de fidélité le fait de poster anonymement sur une plateforme d'évaluation d'entreprises (par exemple, Kununu.com) des remarques sur son employeur et de lui attribuer une note moyenne en fonction de divers critères (conditions et ambiance de travail, intérêt des tâches attribuées, possibilités de formation continue et de promotion, etc.). Notons cependant que le Tribunal cantonal neuchâtelois a considéré que la garantie constitutionnelle de la liberté d'expression pouvait l'emporter suivant les circonstances sur le devoir de réserve des fonctionnaires et a annulé un blâme prononcé à l'encontre d'un enseignant qui était l'auteur d'un message, sur Facebook, de soutien à une manifestation de lycéens[14].

L'employé a l'obligation de maintenir le matériel informatique en bon état, de signaler les défectuosités ou les incidents repérés, et de le protéger contre les risques de détérioration ou les vols[15]. Il respectera aussi les instructions en matière d'utilisation des mots de passe et actionnera régulièrement les mises à jour et antivirus qui lui sont mis à disposition par son employeur[16]. Il ne modifiera pas la configuration matérielle ou logicielle et ne connectera pas sur le réseau de l'entreprise des appareils électroniques non homologués par la direction. L'obligation de restitution vise tous les types de documents, physiques ou informatiques. Elle s'étend par voie de conséquence aux documents scannés que l'employé a transférés de sa messagerie électronique professionnelle à sa messagerie privée[17].

L'étendue du devoir de diligence et de fidélité doit être appréciée dans chaque cas d'espèce en fonction de l'ensemble des circonstances. On prendra en considération le type de travail et la position du travailleur dans l'entreprise[18]. En raison du crédit particulier et de la responsabilité que leur confère leur fonction dans l'entreprise, le compor-

---

11 TF 4C.106/2001 du 14 février 2002, consid. 3c.

12 DUNAND, Commentaire, N 24 ad art. 321*a* CO, p. 60 ; PORTMANN, N 8 ad art. 321*a* CO, p. 1831.

13 STUTZ/GEIGER-STEINER, p. 215. Voir aussi DUNAND, Commentaire, N 16 ad art. 328 CO, p. 275.

14 Arrêt du Tribunal cantonal neuchâtelois, Cour de droit public, du 10 février 2012, dossier n° CDP.2010.45.

15 DUNAND, Commentaire, N 23 ad art. 321*a* CO, p. 60.

16 SUBILIA, p. 56 s.

17 TF 4A_611/2011 du 3 janvier 2012, consid. 4.3.

18 DUNAND, Commentaire, N 6 ad art. 321*a* CO, p. 55.

tement des cadres sera apprécié avec une rigueur accrue[19]. Ainsi, lorsqu'un cadre ne respecte pas les procédures informatiques imposées dans l'entreprise, il risque d'inciter ses subordonnés à croire qu'il s'agit d'un acte banal et qu'ils peuvent procéder de la même façon[20]. Le contenu de l'activité confiée, en particulier dans le domaine bancaire, peut aussi impliquer un rapport de confiance particulièrement solide entre l'employeur et le travailleur[21].

On tiendra également compte de l'instruction ou des connaissances techniques nécessaires pour accomplir le travail, ainsi que des aptitudes et qualités du travailleur[22]. S'agissant de l'usage des moyens informatiques, les exigences seront évidemment plus élevées lorsque le travailleur est informaticien. On examinera aussi les usages propres à chaque profession, ainsi que les directives de l'employeur sur l'accomplissement du travail, les comportements tolérés ou prohibés. Plus celles-ci seront précises et plus facilement pourra être évalué le respect de l'obligation de diligence et de fidélité[23].

B. Utilisation privée d'Internet

L'utilisation d'Internet par le travailleur à des fins privées pose des questions délicates. Après avoir précisé la notion (sous-section 1), nous examinerons les conséquences juridiques de l'autorisation ou, au contraire, de l'interdiction par l'employeur d'une utilisation privée (sous-section 2). Nous traiterons ensuite des quatre critères qui nous paraissent devoir être pris en compte pour évaluer le comportement du travailleur (sous-section 3).

1. Notion

Il faut distinguer l'usage professionnel et l'usage privé d'Internet sur le lieu de travail. L'usage professionnel est celui effectué aux fins de l'exécution d'une prestation de travail ou, plus généralement, à la demande de l'employeur. Toute autre utilisation relève de l'usage privé[24].

Selon de nombreuses études dans divers pays, il est fréquent que des travailleurs effectuent un usage privé d'Internet sur leur lieu de travail. La participation à des réseaux sociaux et à des forums de discussion en ligne (Facebook, LinkedIn, MySpace, Twitter,

19 ATF 130 III 28, consid. 4.1.
20 TF 4A_236/2012 du 2 août 2012, consid. 2.2.
21 TF 4A_236/2012 du 2 août 2012, consid. 2.2.
22 WYLER, p. 107.
23 DUNAND, Commentaire, N 7 ad art. 321*a* CO, p. 55.
24 DUNAND, L'usage de l'Internet, p. 5.

par exemple), la mise en ligne et la gestion de blogs, l'utilisation de plateformes de partage de données (Youtube, par exemple) ou de connaissances (Wikipedia, par exemple) ou encore l'envoi de photos et de vidéos qui s'autodétruisent (Snapchat) figurent parmi les activités en vogue[25]. Dans un cas récemment soumis au Tribunal fédéral, l'on trouve un bon exemple de la palette d'activités possibles. Un programme espion installé pendant plus de trois mois dans l'ordinateur professionnel d'un fonctionnaire tessinois a révélé que celui-ci avait passé environ 70% du temps devant son ordinateur, correspondant à plus de 22% de son temps total de travail, à des activités non professionnelles : lecture de quotidiens online, participation à des réseaux sociaux, vision de films TV et d'autres films (parfois à contenu érotiques) online ; exécution de jeux et d'opérations d'e-banking, réservation de voyages, envoi de courriels privés, téléchargement de fichiers privés pour ses propres activités politiques ou récréatives[26].

La distinction entre usage professionnel et usage privé n'est toutefois pas toujours aussi évidente[27]. Il n'est pas rare que l'employeur « offre » l'usage d'un smartphone ou d'une tablette électronique comme « cadeau de bienvenue » à ses employés. L'appareil sera utilisé autant pour les activités professionnelles du travailleur que pour ses activités privées. La pratique du BYOD est inverse mais pose les mêmes problèmes de confusion des sphères privée et professionnelle. Par ailleurs, il est très fréquent qu'un collègue de travail, un partenaire commercial, ou toute autre personne avec qui le travailleur est en relation professionnelle, fasse également partie de son cercle d'amitié. Il en résulte une relation hybride, à la fois professionnelle et privée, qui se répercute nécessairement sur le mode et le contenu des communications. Ainsi, des courriers électroniques sont susceptibles de contenir aussi bien des communications professionnelles que des communications privées. Il peut arriver aussi que des collègues, même de niveau hiérarchique différent, soient « amis » sur les réseaux sociaux[28]. Cette réalité est peu compatible avec la volonté de séparer clairement ce qui relève de la sphère professionnelle et de la sphère privée.

2. Utilisation privée autorisée ou interdite

Conséquence de lien de subordination existant entre les parties, l'employeur est en droit de donner des directives à ses employés sous la forme de directives générales ou

25 Voir EGLI, ainsi que la contribution dans le présent ouvrage de CAROLE AUBERT et RÉGINE DELLEY consacrée à l'utilisation des réseaux sociaux (p. 133 ss).

26 ATF 139 II 7, faits de la cause (lettre A.), JdT 2013 II 188 (rés.), SJ 2013 I 177 (rés.). Notons que le licenciement immédiat de ce collaborateur a été annulé au motif que la preuve des manquements, obtenue de manière illégale, a été écartée (cf. consid. 5 à 7).

27 ALDER, p. 277 ; DUNAND, L'usage de l'Internet, p. 5.

28 EGLI, N 87 ss.

d'instructions particulières qui peuvent être adaptées ou modifiées au gré des circonstances (art. 321*d* al. 1 CO). L'employeur peut évidemment réglementer par ce biais l'usage d'Internet et de la messagerie électronique par ses employés. Le travailleur est tenu d'observer « selon les règles de la bonne foi les directives générales et instructions particulières qui lui ont été données » par l'employeur (art. 321*d* al. 2 CO).

Il est admis que l'employeur a la possibilité d'interdire toute utilisation d'Internet ou de la messagerie professionnelle à des fins privées[29]. Une telle interdiction peut évidemment comporter des avantages pour l'entreprise en ce qui concerne notamment la gestion du temps de travail et la sécurité des données[30]. Une interdiction totale ne constitue toutefois pas toujours la mesure la plus opportune en termes de gestion du personnel[31]. Elle posera en outre des difficultés de mise en œuvre, car comme nous le verrons les possibilités de surveiller l'utilisation, d'apporter la preuve d'un manquement et de sanctionner le travailleur sont juridiquement délicates. Il est dès lors compréhensible qu'en pratique la plupart des entreprises autorisent ou tolèrent un usage privé raisonnable, ne serait-ce que pendant le temps de pause. L'employeur pourra exiger que les employés indiquent expressément la nature privée des courriels sortants par l'indication du mot « privé » ou « personnel » dans la rubrique consacrée à l'objet du message[32]. En tous les cas, l'employeur devra partir du principe que tout courriel signalé comme tel (avec la mention « privé » ou « personnel ») ou dont le titre est suffisamment éloquent (par exemple, l'utilisation du mot « Schatzi » !) est exclusivement de nature privée[33][34].

En l'absence de directives ou d'indications contraires de l'employeur, il ne nous semble pas que l'on puisse considérer que toute utilisation privée d'Internet constitue une violation du devoir de diligence et de fidélité du travailleur. Certes, la plupart des travailleurs possèdent leurs propres moyens de communication électroniques qu'ils peuvent utiliser sans mettre à contribution l'infrastructure de l'entreprise[35]. Le travailleur doit cependant se voir reconnaître, dans une certaine mesure, le droit de communiquer à l'intérieur et à l'extérieur de l'entreprise par le biais des moyens informatiques qui sont mis à sa disposition[36]. Le travailleur peut ainsi partir du principe qu'un usage privé raisonnable et

---

29 TF 4A_430/2008 du 24 novembre 2008, consid. 4 ; BRUNNER/BÜHLER/WAEBER/BRUCHEZ, N 5 ad art. 328 CO, p. 142 ; Meier, N 2170, p. 701 et N 2198, p. 710 ; STREIFF/VON KAENEL/RUDOLPH, N 17 ad art. 328*b* CO, p. 619.

30 ADLER, p. 277.

31 MEIER, N 2171, p. 702 et N 2198, p. 710.

32 AUBERT, N 9 ad art. 328*b* CO, p. 2030 s.

33 Voir le jugement du Tribunal arbitral des prud'hommes de Bâle-Ville du 29 janvier 2001, in : JAR 2004, p. 440.

34 CARRUZZO, N 23 ad art. 328*b* CO, p. 343.

35 ALDER, p. 277 ; EGLI, N 40 ; STREIFF/VON KAENEL/RUDOLPH, N 17 ad art. 328*b* CO, p. 619 s.

36 GEISER, Die Beaufsichtigung, p. 206 ss ; HOLENSTEIN, p. 46 s. et 82.

proportionné d'Internet et de la messagerie est toléré pour autant évidemment qu'il ne porte pas atteinte aux intérêts légitimes de l'employeur[37]. Cela peut comprendre, par exemple, la consultation sporadique du site web d'un journal d'informations ou l'envoi de deux à trois courts messages par jour[38]. Pour éviter toute ambiguïté, le travailleur identifiera clairement les courriels sortants avec la mention « privé »[39].

3. Critères déterminants

Finalement, que l'usage d'Internet soit expressément autorisé, simplement toléré, ou interdit, la qualification des actes du travailleur et leur sanction devra s'effectuer en tenant compte des quatre critères suivants : la prestation de travail (a), les coûts financiers (b), la sécurité et la réputation de l'entreprise (c), et enfin, la nature des sites visités (d)[40].

a) Prestation de travail

Selon l'article 319 al. 1 CO, le travailleur s'engage essentiellement à mettre sa force de travail au service de son employeur. Pendant le temps de travail convenu, et à défaut d'accord contraire, le travailleur a l'obligation d'exercer toute son activité en faveur de son employeur, et non pas en faveur d'un tiers ou pour lui-même (cf. aussi art. 321*a* al. 1 CO). Comme le relève Gabriel Aubert, le « travailleur est payé pour travailler [CO 319 I] et non pas pour conduire des conversations téléphoniques privées, pour surfer à loisir sur Internet ou pour envoyer des messages électroniques personnels au moyen des installations de l'employeur et aux frais de ce dernier »[41]. Il résulte des principes généraux que lorsque le travailleur qui est apte au travail ne fournit pas sa prestation, il est en demeure. Il perd en principe son droit au salaire (cf. art. 82, 119, 319 et 324*a* CO)[42]. Suivant les circonstances, le travailleur qui s'est adonné à des activités privées pendant ses heures de travail pourrait donc se voir opposer une réduction de son salaire.

La question doit cependant aussi être analysée dans un contexte plus général : celui de l'exécution correcte et efficace de la prestation de travail. Celui qui surfe généreusement sur Internet pendant les heures de travail se trouve dans la même position que le travailleur qui bavarde assidûment ou prend des pauses trop longues et trop nombreuses pour

---

37 BRUNNER/BÜHLER/WAEBER/BRUCHEZ, N 5 ad art. 328 CO, p. 142 s. ; EGLI, N 33 ss ; MEIER, N 2182, p. 704 s. et N 2202, p. 711 ; VON KAENEL, Internet, p. 43.

38 STREIFF/VON KAENEL/RUDOLPH, N 17 ad art. 328*b* CO, p. 621.

39 MEIER, N 2183, p. 705.

40 DUNAND, L'usage de l'Internet, p. 7 ss ; HOLENSTEIN, p. 82 ss.

41 AUBERT, N 8 ad art. 328*b* CO, p. 2030.

42 CARRUZZO, N 2 ad art. 324*a* CO, p. 195.

boire des cafés, fumer des cigarettes ou aller aux toilettes. Dans la pesée des intérêts en cause, il faudra apprécier la qualité des prestations du travailleur. Un employé efficace et diligent dans son travail ne saurait être évalué ou sanctionné de la même manière qu'un employé démotivé et aux prestations médiocres. Il sera, par exemple, plus difficile de reprocher un manquement à un travailleur excellent du fait qu'il a passé cinq minutes par jour sur Internet pendant son temps de travail à consulter un site d'informations sportives.

Il faut aussi tenir compte du fait que certaines activités sur Internet, bien que de nature privée, peuvent avoir des répercussions positives sur la prestation de travail lorsqu'elles permettent l'acquisition d'un savoir-faire susceptible de profiter également à l'entreprise[43]. Les employés qui ont recours aux moyens informatiques travaillent généralement de manière plus indépendante. On a pu remarquer que le développement de l'informatique avait favorisé une organisation de travail différente dans l'entreprise au sein de laquelle l'activité du travailleur est moins évaluée selon le temps de travail effectif que selon le résultat fourni. En conséquence, l'obligation du travailleur de consacrer tout son temps de travail à l'exécution des tâches assignées par l'employeur et non à des activités privées s'en trouverait, dans certains cas, relativisée[44].

b) Coûts financiers

Comme tout autre instrument de travail, l'employeur fournit en principe au travailleur le matériel dont celui-ci a besoin pour exécuter son travail (cf. art. 327 al. 1 CO). L'utilisation du matériel et du réseau informatique engendre nécessairement des coûts (connexion, électricité, impression de textes, etc.) Lorsque les coûts de connexion sont calculés selon un tarif forfaitaire, la durée de la connexion à Internet n'a en principe pas d'incidence. En revanche, lorsque les coûts sont facturés à l'entreprise en fonction du temps et/ou du volume ou de la distance, la durée effective et le volume data des connexions influent sur les coûts. A moins qu'ils ne soient dérisoires, le travailleur pourrait être tenu de prendre en charge les frais qu'il a engendrés par une utilisation privée d'Internet[45].

Une utilisation non professionnelle d'Internet par le travailleur est cependant susceptible de générer des pertes ou des coûts bien plus importants à la charge de l'employeur. On pensera par exemple à la paralysie du réseau informatique impliquant une impossibilité de travail pour de nombreux collaborateurs en raison de l'introduction d'un virus ou de l'atteinte à la capacité de stockage et à la bande passante du réseau de l'entreprise. On

43 HOLENSTEIN, p. 37 s.
44 DUNAND, L'usage de l'Internet, p. 10.
45 VON KAENEL, Internet, p. 41 s.

mentionnera aussi les activités qui contreviennent aux règles sur la protection et la sécurité des données et celles sur le droit d'auteur, comme le fait de copier illégalement des logiciels, de diffuser des informations confidentielles ou de ne pas mentionner les sources lors de l'utilisation d'informations provenant de tiers, ou encore les activités qui portent atteinte aux droits la personnalité de collègues ou de tiers. Selon les règles générales, l'employeur devra répondre des actes de ses organes ou de ses auxiliaires (cf. art. 55 CC, 55 CO et 101 CO).

Ces divers comportements constituent des manquements du travailleur qui, comme nous le verrons, pourront fonder, suivant les cas, une action en responsabilité (cf. art. 321*e* CO) et/ou un licenciement immédiat (cf. art. 337 CO) des travailleurs concernés.

c) Sécurité, confidentialité et réputation de l'entreprise

Toute connexion à Internet par le travailleur est de nature à porter gravement atteinte à la sécurité et à la confidentialité des activités de l'entreprise. On pensera en particulier aux usages qui outrepassent les capacités de mémoire ou qui contribuent à introduire dans le réseau de l'entreprise des virus, vers, ou autre « cheval de Troie » susceptibles de détruire des données, paralyser le réseau informatique ou créer un accès indu aux données informatiques depuis l'extérieur[46].

Chaque accès à Internet laisse des traces sur le réseau informatique. L'identité de l'entreprise depuis laquelle la connexion a été effectuée peut être identifiée comme source de communication[47]. La réputation, la sécurité et la confidentialité de ses activités peuvent s'en trouver affectées[48]. Une mauvaise utilisation d'Internet peut aussi provoquer l'enregistrement de l'adresse de l'employeur dans des sites externes commerciaux qui diffuseront des informations non désirées, soit chez le travailleur, voire chez tous les employés de l'entreprise.

Les employés, qui seront rendus attentifs à ces risques, pourront être sanctionnés en cas de manquement. La jurisprudence est toutefois plutôt compréhensive à l'égard des travailleurs. Ainsi, le Tribunal fédéral s'est penché sur une affaire dans laquelle il fallait notamment déterminer si le travailleur avait porté atteinte à la réputation de son entreprise. L'employé d'une entreprise informatique avait adressé divers messages électroniques ayant un contenu pornographique à plusieurs personnes, dont une connaissance travaillant auprès d'un autre employeur. Les messages destinés à cette connaissance, absente de son lieu de travail pour cause de service militaire, avaient été automatique-

46 MONDINI, p. 364 ; SUBILIA, p. 58.
47 STREIFF/VON KAENEL/RUDOLPH, N 17 ad art. 328*b* CO, p. 620.
48 HOLENSTEIN, p. 44 ss ; VON KAENEL, Internet, p. 42.

ment transférés sur la messagerie de l'un de ses collègues de travail, lequel avait alerté son supérieur hiérarchique. Celui-ci avait alors recherché et trouvé l'adresse émettrice des messages, puis informé l'entreprise informatique de l'identité de l'expéditeur. Selon le Tribunal fédéral, le comportement du travailleur était, certes, inacceptable, mais il ne constituait pas une grave violation des obligations résultant du contrat de travail. Notre Haute Cour a encore considéré que le message était adressé à une personne consentante et que le risque qu'il soit transféré à une autre personne devait sans doute être pris en compte par l'expéditeur, mais qu'on ne pouvait lui reprocher qu'un comportement négligent. Par ailleurs, toujours selon le Tribunal fédéral, dans la mesure où le travailleur n'était pas un cadre ni un représentant de l'entreprise, ses agissements n'étaient pas de nature à porter véritablement atteinte à la réputation de son employeur[49].

d) Contenu

Il faut enfin tenir compte d'une appréciation qualitative, eu égard au contenu (nature des sites visités, contenu des messages électroniques) de l'utilisation privée d'Internet par le travailleur. Le travailleur est évidemment tenu de respecter les dispositions impératives du droit suisse, et en particulier de ne pas contrevenir aux normes pénales. Il faut relever que de nombreuses infractions pénales sont susceptibles d'être commises par le biais d'une utilisation abusive d'Internet[50].

Il va de soi que toute infraction pénale commise au détriment de l'employeur est une violation grave du devoir de fidélité susceptible de fonder un licenciement immédiat[51]. En pratique, c'est souvent la consultation de sites à contenu pornographique qui est problématique. Lorsque la consultation de tels sites ou l'envoi de messages électroniques de contenu similaire contreviennent au Code pénal suisse, en particulier à l'article 197 chiffre 3bis, le manquement doit être considéré comme grave, ce qui justifie en principe un licenciement immédiat au sens de l'art. 337 CO[52].

En revanche, selon le Tribunal fédéral, une consultation peu fréquente de sites pornographiques ne constitue en principe pas une violation grave du devoir de fidélité qui justifierait un licenciement immédiat sans avertissement préalable : « Es ist aber ebenso zutreffend, dass eine private Internetbenützung am Arbeitsplatz während der Arbeitszeit, falls sie sich auf wenige Male beschränkt, eine fristlose Entlassung ohne vorgängige Verwar-

49 TF 4C.109/2003 du 30 juillet 2003, consid. 2.2.2.
50 MOREILLON, p. 21 ss ; STOLL, p. 111 ss.
51 GLOOR, N 40 ad art. 337 CO, p. 752.
52 TF 4C.109/2003 du 30 juillet 2003, consid. 2.2.1.

nung nicht zu rechtfertigen vermag, selbst wenn der Arbeitnehmer wie im vorliegenden Fall Sexseiten angeschaut haben sollte »[53].

C. Responsabilité du travailleur (art. 321*e* CO)

Selon l'article 321*e* al. 1 CO, le travailleur « répond du dommage qu'il cause à l'employeur intentionnellement ou par négligence ». Comme toute responsabilité contractuelle, la responsabilité du travailleur suppose la réalisation de quatre conditions cumulatives, à savoir un dommage, la violation d'une obligation contractuelle, un lien de causalité entre ladite violation et le dommage, ainsi qu'une faute. Lorsque ces conditions sont réalisées, la responsabilité du travailleur pourra être engagée, qu'il s'agisse d'une utilisation professionnelle ou privée d'Internet.

La violation contractuelle pourra consister, par exemple, dans l'introduction d'un virus dans le système parce que l'employé a téléchargé un logiciel depuis un site non autorisé ou parce qu'il n'a pas mis à jour l'antivirus malgré des instructions de l'employeur[54]. Quant au dommage subi par l'employeur, il pourra résulter des frais de réparation ou de remplacement d'ordinateurs, de programmes ou de fichiers, de la perte de gain liée à la destruction de données ou à l'endommagement du réseau, ou encore des montants payés à des tiers du fait de la responsabilité contractuelle ou extracontractuelle de l'employeur (action récursoire contre le travailleur).

Selon l'article 321*e* alinéa 2 CO, la « mesure de la diligence incombant au travailleur se détermine par le contrat, compte tenu du risque professionnel, de l'instruction ou des connaissances techniques nécessaires pour accomplir le travail promis, ainsi que des aptitudes et qualités du travailleur que l'employeur connaissait ou aurait dû connaître ». Le Tribunal fédéral a précisé que l'article 321*e* al. 2 CO ne contenait pas une liste exhaustive de facteurs de réduction, si bien que d'autres éléments, comme l'attitude du travailleur, pouvaient intervenir[55].

L'étendue de la réparation se mesure selon les circonstances et la gravité de la faute de l'employé (cf. art. 43 al. 1 et art. 321*e* al. 2 CO), compte tenu d'une éventuelle faute concomitante de l'employeur (cf. art. 44 al. 1 CO). En pratique, les critères principaux pour fixer l'indemnité résident dans la quotité du salaire, la gravité de la faute (cf. art. 43 al. 1 CO) et le risque professionnel[56]. En cas de faute légère, le travailleur est souvent

53 TF 4C.349/2002 du 25 juin 2003, consid. 5.
54 SUBILIA, p. 56.
55 TF 4A_123/2007 et 4A_125/2007 du 31 août 2007, consid. 8.2.
56 DUNAND, Commentaire, N 38 ad art. 321*e* CO, p. 130.

libéré de toute obligation de réparer le préjudice causé[57]. La mesure de la diligence requise du travailleur s'apprécie en premier lieu selon le contrat de travail, y compris les prescriptions contenues dans un règlement d'utilisation des moyens informatiques. Le juge tiendra compte en second lieu du risque professionnel, qui découle du haut degré de probabilité de survenance d'un dommage. Le risque professionnel incombe à l'employeur[58]. Certains dommages sont inhérents à l'activité ; d'autres peuvent découler des matériaux utilisés, ainsi que de la méthode ou du rythme de travail dans l'entreprise[59]. Tout employé qui utilise fréquemment des moyens informatiques est confronté à des risques, par exemple d'introduire un virus dans son ordinateur ou d'adresser par erreur un courrier électronique à un destinataire non souhaité.

L'existence d'une faute concomitante de l'employeur constitue également un motif de réduction des dommages-intérêts dus par le travailleur. Sera, par exemple, considéré comme fautif l'employeur qui a fourni du matériel ou des instruments de travail défectueux ou non adaptés à la prestation exigée du travailleur (par exemple, ordinateur dépourvu de filtres ou de logiciels antivirus adaptés)[60]. Il en va de même lorsque l'employeur a mal organisé le travail (par exemple, plusieurs administrateurs système du même ordinateur), a assigné un travail non approprié, n'a pas donné les instructions utiles (par exemple, en matière de gestion des mots de passe) ou n'a pas contrôlé l'exécution du travail et le respect des instructions de manière adéquate[61].

D. Licenciement avec effet immédiat (art. 337 CO)

Le licenciement immédiat d'un travailleur ayant commis un manquement grave à son devoir de diligence et de fidélité lors de l'utilisation des moyens informatiques est envisageable. Il s'agit de rappeler les principes généraux du licenciement pour de justes motifs (sous-section 1) avant de présenter la jurisprudence du Tribunal fédéral en matière d'utilisation abusive de l'ordinateur (sous-section 2).

57 DUNAND, Commentaire, N 42 ad art. 321*e* CO, p. 131.
58 DUNAND, Commentaire, N 30 ad art. 321*e* CO, p. 127.
59 BRUNNER/BÜHLER/WAEBER/BRUCHEZ, N 5 ad art. 321*e* CO, p. 77.
60 BRUNNER/BÜHLER/WAEBER/BRUCHEZ, N 4 ad art. 321*e* CO, p. 77.
61 TF 4C.103/2005 du 1er juin 2005, consid. 1.3 ; TF 4C.87/2001 du 7 novembre 2001, consid. 4b ; Tribunal cantonal fribourgeois du 14 septembre 2006, consid. 2a, in : JAR 2007, p. 400 ; AUBERT, N 5 ad art. 321*e* CO, p. 1986 ; SUBILIA, p. 56 ss.

1. Principes

Selon l'article 337 al. 1 CO, l'employeur et le travailleur peuvent résilier le contrat de travail en tout temps pour de justes motifs. Doivent notamment être considérés comme tels toutes les circonstances qui, selon les règles de la bonne foi, ne permettent pas d'exiger de celui qui a donné le congé la continuation des rapports de travail (cf. art. 337 al. 2 CO). Mesure exceptionnelle, la résiliation immédiate pour justes motifs doit être admise de manière restrictive ; d'après la jurisprudence, les faits invoqués à l'appui d'un renvoi immédiat doivent avoir entraîné la perte du rapport de confiance qui constitue le fondement du contrat de travail ; seul un manquement particulièrement grave du travailleur justifie son licenciement immédiat ; si le manquement est moins grave, il ne peut entraîner une résiliation immédiate que s'il a été répété malgré un avertissement ; par manquement, on entend en règle générale la violation d'une obligation découlant du contrat de travail, mais d'autres incidents peuvent aussi justifier une résiliation immédiate[62]. Le juge apprécie librement s'il existe de justes motifs (art. 337 al. 3 CO). Il applique les règles du droit et de l'équité (art. 4 CC). A cet effet, il prendra en considération tous les éléments du cas particulier, notamment la position et la responsabilité du travailleur, le type et la durée des rapports contractuels, ainsi que la nature et l'importance des manquements[63].

2. Jurisprudence sur l'usage abusif des moyens informatiques

Le Tribunal fédéral a montré jusqu'ici une certaine clémence envers les travailleurs ayant abusé des moyens de communication électronique dans leur entreprise. Nous ferons une synthèse de la jurisprudence en distinguant les licenciements immédiats qui ont été considérés comme injustifiés (a) de ceux dont notre Haute Cour a admis la validité (b).

a) Licenciements immédiats injustifiés

– Le fait d'échanger sur le système informatique de l'employeur, avec deux collègues de travail, divers messages personnels contenant des réflexions vulgaires ne justifie pas un licenciement immédiat, lorsqu'il a été établi que bon nombre de collaborateurs et même des membres de la direction de la société, active dans le courtage en assurance et réassurance, avaient coutume de formuler, en s'adressant à des collègues ou à des subordonnés, des réflexions à connotation sexuelle, parfaitement déplacées[64].

---

62 ATF 130 III 28, consid. 4.1 ; GLOOR, N 22 ad art. 337 CO, p. 742 s.

63 ATF 130 III 28, consid. 4.1 ; ATF 129 III 380, consid. 2 ; ATF 127 III 351, consid. 4a ; GLOOR, N 24 et 25 ad art. 337 CO, p. 743 s.

64 TF 4C.463/1999 du 4 juillet 2000, consid. 9f.

– Le fait de jouer aux cartes sur son ordinateur, et de laisser ou de réinstaller des jeux sur son propre ordinateur, alors que l'employeur avait prié l'employé de les faire enlever sur tous les postes de travail de l'entreprise sont, selon le Tribunal fédéral, des manquements de moindre gravité, qui en principe ne justifient un licenciement immédiat du travailleur, en l'occurrence « responsable du poste de Directeur Gestion-Finance », que s'ils ont été précédés d'un avertissement[65].
– De même, ne fonde pas un renvoi immédiat du travailleur, engagé en qualité de « Logistic Engineer », un usage privé d'Internet sur le lieu de travail, lorsqu'il s'agit de quelques utilisations, même quand le site consulté a une connotation sexuelle[66].
– Ne justifie toujours pas un licenciement immédiat le fait d'adresser divers messages électroniques à connotation sexuelle à plusieurs personnes, collègues ou collaborateurs d'autres entreprises, même si l'un de ces messages a été transféré à une personne non prévue, suite à l'absence pour cause de service militaire du destinataire travaillant dans une autre entreprise, et que l'existence de ce message a été communiqué par un cadre de cette entreprise à l'employeur du travailleur congédié avec effet immédiat[67].
– Enfin, l'employeur ne saurait se prévaloir de faits qu'il a tolérés. Selon le Tribunal fédéral, la résiliation immédiate est notamment soumise à la condition que l'employeur ne connaissait pas et ne pouvait pas connaître les faits constitutifs des justes motifs. Tel n'est pas le cas lorsqu'il savait que l'employé fréquentait avec une certaine assiduité des sites Internet à des fins privées et qu'il n'a pas réagi[68].

b) Licenciement immédiats justifiés

– Constitue un juste motif de licenciement immédiat le fait de se ménager un accès à la messagerie électronique de son patron, permettant au travailleur de consulter, aussi bien au bureau qu'à la maison, sous son propre nom d'utilisateur et mot de passe, les courriels parvenant à cette adresse. Dans le cas soumis au Tribunal fédéral, relatif à une entreprise active dans le secteur de l'industrie graphique, il n'a pas été possible de constater si le travailleur avait pris connaissance des messages à caractère privé adressés à son directeur ou, a fortiori, qu'il avait divulgué les informations s'y trouvant. Le Tribunal fédéral a cependant estimé que le seul fait de s'être ménagé la possibilité d'y avoir accès librement portait déjà atteinte au secret des communications, garanti à l'article 13 de la Constitution fédérale, et constituait une violation de la

65 TF 4C.106/2001 du 14 février 2002, consid. 3c.
66 TF 4C.349/2002 du 25 juin 2003, consid. 5.
67 TF 4C.109/2003 du 30 juillet 2003, consid. 2.
68 TF 4C.173/2003 du 21 octobre 2003, consid. 3.2.

sphère intime du directeur, contraire au droit au respect de sa vie privée, garanti à l'article 28 du Code civil, voire une infraction pénale au sens de l'article 143bis du Code pénal[69].

– Constituent également de justes motifs pour un congé abrupt le fait, pour une responsable d'un département d'une banque, de donner ses codes informatiques à ses subordonnés en violation d'une obligation essentielle imposée par l'employeur, et ceci pendant une période d'environ trois ans, de ne pas respecter la procédure de « call back », de ne pas contrôler le journal des opérations et de dissimuler ses absences[70].

III. Obligations et responsabilité de l'employeur

L'ordinateur, ainsi que les ondes, images ou messages qu'il véhicule font courir à l'employé des risques d'atteinte à sa personnalité et à sa santé contre lesquels l'employeur doit le protéger. Après avoir rappelé les principes généraux relatifs à la protection de la personnalité (section A), nous traiterons de trois types d'atteinte fréquente par le biais d'Internet et de la messagerie électronique, à savoir l'exigence d'être continuellement disponible (section B), le harcèlement (section C) et la violation des règles sur la protection des données (section D). Nous conclurons par une synthèse des règles sur la responsabilité de l'employeur (section E).

A. Devoir de protection de la personnalité : principes généraux

Selon l'article 328 al. 1 CO, l'employeur « protège et respecte, dans les relations de travail, la personnalité du travailleur ; il manifeste les égards voulus pour sa santé et veille au maintien de la moralité. En particulier, il veille à ce que les travailleurs ne soient pas harcelés sexuellement et qu'ils ne soient pas, le cas échéant, désavantagés en raison de tels actes ». La protection couvre l'ensemble des valeurs essentielles, physiques, affectives et sociales liées à la personne humaine[71]. 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[72]. Il est admis que l'employeur doit non seulement respecter la personnalité du travailleur, mais aussi la

69 ATF 130 III 28, consid. 4.
70 TF 4A_236/2012 du 2 août 2012, consid. 2.3.
71 TF 2C_103/2008 du 30 juin 2008, consid. 6.2.
72 BRUNNER/BÜHLER/WAEBER/BRUCHEZ, N 2 ad art. 328 CO, p. 141.

protéger. Il doit donc autant s'abstenir de porter directement atteinte aux droits de la personnalité de ses employés que de prendre des mesures adéquates pour empêcher qu'ils ne subissent une telle atteinte[73]. L'employeur doit notamment veiller à ce que ses employés puissent exécuter leur prestation de travail dans des conditions qui respectent leur personnalité[74].

Selon l'article 328 al. 2 CO, l'employeur doit prendre, « pour protéger la vie, la santé et l'intégrité personnelle du travailleur, les mesures commandées par l'expérience, applicables en l'état de la technique, et adaptées aux conditions de l'exploitation ou du ménage, dans la mesure où les rapports de travail et la nature du travail permettent équitablement de l'exiger de lui ». La norme vise tous les risques liés à l'exploitation de l'entreprise. L'employeur doit non seulement prévenir les accidents du travail, mais aussi, plus généralement, toutes les atteintes à la santé pouvant résulter de l'exécution du travail[75].

L'obligation de l'employeur de protéger la santé de ses employés découle autant de l'art. 328 CO que des règles de droit public qui s'appliquent selon le champ d'application respectif des lois concernées (cf. art. 6 LTr et art. 82 LAA). Ainsi, selon l'art. 6 al. 1 LTr, l'employeur est tenu pour protéger la santé des travailleurs de « prendre toutes les mesures dont l'expérience a démontré la nécessité, que l'état de la technique permet d'appliquer et qui sont adaptés aux conditions d'exploitation de l'entreprise ». Diverses précautions doivent être prises pour les travailleurs utilisant quotidiennement un ordinateur. Par exemple, selon l'art. 2 al. 1 OLT 3, l'employeur est tenu de prendre toutes les mesures nécessaires afin d'assurer et d'améliorer la protection de la santé et de garantir la santé physique et psychique des travailleurs. Il doit en particulier faire en sorte que les conditions de travail soient bonnes en matière ergonomique et d'hygiène (lettre a), que des efforts excessifs ou trop répétitifs soient évités (lettre c), ou encore que le travail soit organisé de façon appropriée (lettre d).

B. Disponibilité continue

Nous avons vu que l'utilisation des moyens informatiques associée aux nouvelles technologies rendait moins claire les notions de lieu et de temps de travail. Il est par exemple devenu usuel pour de nombreux travailleurs de consulter leur messagerie professionnelle voir certains fichiers accessibles on-line pendant les pauses, jours de congé, vacances ou

---

73 TF 4A_128/2007 du 9 juillet 2007, consid. 2.2 ; BRUNNER/BÜHLER/WAEBER/BRUCHEZ, N 2 ad art. 328 CO, p. 141 ; SONNENBERG, p. 67 ss.

74 DUNAND, Commentaire, N 20 ad art. 328 CO, p. 276.

75 ATF 132 III 257, consid. 5.2., JdT 2007 I 274, SJ 2007 I 173.

périodes d'incapacité de travail, et quel que soit le lieu où ils se trouvent. La pratique du BYOD par laquelle le travailleur utilise ses propres appareils électroniques contribue au développement de ce processus de disponibilité continue puisqu'elle crée une perméabilité entre activité professionnelle et activité privée[76]. Souvent, l'utilisation de la messagerie s'opère à l'initiative de l'employé qui souhaite être informé des derniers développements, rester compétitif, prendre de l'avance dans son travail ou tout simplement plaire à son employeur. Parfois, la disponibilité continue impliquant d'être connecté ou joignable presque tous les jours de l'année est une obligation imposée par l'employeur. Une telle exigence comporte un risque important de violation de règles impératives du droit du travail (protection de la personnalité et de la santé, horaires de travail, etc.).

Il résulte de l'article 328 CO et de l'article 6 LTr que l'employeur doit ménager l'intégrité de ses employés en s'abstenant de leur demander des efforts excessifs et de les charger de travaux pouvant porter atteinte ou mettre en danger leur santé[77]. Il doit aussi organiser le travail de manière à éviter un stress inutile[78]. Exiger une disponibilité quasi permanente d'un travailleur contrevient clairement à ce devoir de protection[79].

Selon l'article 329 al. 1 CO, l'employeur doit accorder au travailleur un jour de congé par semaine, en règle générale le dimanche. Le but du congé hebdomadaire est de protéger la santé du travailleur. Pendant le congé hebdomadaire, l'employeur n'a aucune prétention à l'obtention de la prestation de travail[80]. L'employeur doit en outre accorder au travailleur, selon l'article 329*a* al. 1 CO, chaque année de service, quatre semaines de vacances au moins et cinq semaines au moins aux travailleurs jusqu'à l'âge de 20 ans révolus. Le but des vacances est de permettre au travailleur de se reposer et de se détendre. Comme le relève Cerottini, les « vacances constituent une période durant laquelle le travailleur doit pouvoir prendre de la distance à l'égard de ses obligations professionnelles, se reposer sans se soucier de son travail. A ce titre, il n'existe pas […] de devoir contractuel pour le travailleur de rester atteignable durant ses vacances. Admettre le contraire reviendrait en effet à limiter dans une trop grande mesure la liberté de choix des activités qu'il entend mener pendant les vacances »[81].

Selon l'art. 46 LTr, l'employeur soumis à la législation sur le travail doit tenir à disposition des autorités compétentes les registres ou autres pièces contenant les informations

76 Voir la contribution de SÉBASTIEN FANTI dans le présent ouvrage.
77 DUNAND, Commentaire, N 14 ad art. 328 CO, p. 275.
78 DUNAND, Commentaire, N 45 ad art. 328 CO, p. 287.
79 VON KAENEL, Erreichbarkeit, p. 2 ss.
80 CEROTTINI, N 6 ad art. 329 CO, p. 358.
81 CEROTTINI, N 2 ad art. 329*a* CO, note 2, p. 368.

nécessaires à l'exécution de la Loi sur le travail et de ses ordonnances[82]. L'article 73 al. 1 OLT 1 précise que les registres et pièces comportent toutes les données nécessaires à l'exécution de la loi. Cela comprend notamment les durées (quotidienne et hebdomadaire) du travail fourni (lettre c), les jours de repos ou de repos compensatoire hebdomadaire accordés, pour autant qu'ils ne tombent pas régulièrement un dimanche (lettre d), ainsi que l'horaire et la durée des pauses d'une durée égale ou supérieure à une demi-heure (lettre e). L'obligation de documenter les données permet notamment de déterminer le temps de travail effectif et de vérifier le respect des prescriptions sur le travail supplémentaire (cf. art. 12 et 13 LTr), le travail de nuit (art. 16 ss LTr) et le travail le dimanche (art. 18 ss LTr)[83].

La violation des dispositions susmentionnées peut impliquer diverses sanctions à l'encontre de l'employeur comme l'obligation de payer les heures supplémentaires (cf. art. 321*c* al. 3 CO) ou le travail supplémentaire (cf. art. 13 LTr) accompli, de verser des dommages-intérêts (cf. art. 97 et 328 CO) ou de compenser les jours de congé ou de vacances dont l'employé n'a pas pu véritablement profiter. Suivant les cas, le travailleur devrait aussi pouvoir réclamer le paiement des heures pendant lesquelles il était simplement à disposition de l'employeur, à un tarif horaire réduit, par analogie avec le régime juridique applicable en matière de travail sur appel[84]. Au vu de ce qui précède, l'employeur doit absolument encadrer juridiquement le devoir d'être accessible en dehors des heures usuelles de travail, par une convention conforme aux règles impératives, ou alors renoncer à une telle pratique[85].

C. Harcèlement

Le harcèlement constitue souvent la manifestation insidieuse d'une volonté de domination et de manipulation d'un individu par un autre[86]. L'utilisation des moyens informatiques peut favoriser les actes de harcèlement[87]. Il est d'ailleurs fréquent que tout ou partie d'un harcèlement sur le lieu de travail s'opère par un usage illicite des moyens

82 RUDOLPH/VON KAENEL, p. 204 ss. Voir aussi la Directive du SECO concernant les contrôles de l'enregistrement de la durée du travail (art. 46 LTr et 73 de l'ordonnance 1 relative à la LTr) – à appliquer à partir du 1.1.2014, Berne, décembre 2013.

83 VON KAENEL, Erreichbarkeiz, p. 5 ss.

84 RUDOLPH/VON KAENEL, p. 207 ; VON KAENEL, Erreichbarkeit, p. 7.

85 VON KAENEL, Erreichbarkeit, p. 9.

86 DEVEAUD-PLÉDRAN, p. 15.

87 BAUMGARTNER, p. 1435.

informatiques[88]. Nous distinguerons le harcèlement psychologique (sous-section 1) du harcèlement sexuel (sous-section 2).

1. Harcèlement psychologique

Le harcèlement psychologique constitue une atteinte grave à la personnalité, et souvent à la santé, du travailleur. En l'absence d'une norme légale spécifique, la notion a été précisée par la doctrine[89] et la jurisprudence[90]. Selon la définition qu'en donne le Tribunal fédéral, « le harcèlement psychologique, appelé aussi mobbing, se définit comme un enchaînement de propos et/ou d'agissements hostiles, répétés fréquemment pendant une période assez longue, par lesquels un ou plusieurs individus cherchent à isoler, à marginaliser, voire à exclure une personne de son lieu de travail. […]. La victime est souvent placée dans une situation où chaque acte pris individuellement, auquel un témoin a pu assister, peut éventuellement être considéré comme supportable alors que l'ensemble des agissements constitue une déstabilisation de la personnalité, poussée jusqu'à l'élimination professionnelle de la personne visée »[91]. Les comportements hostiles portent généralement sur les relations sociales de la victime, la considération dont elle bénéficie, la qualité de sa vie professionnelle et de sa vie privée, ainsi que sa santé[92]. Les actes de harcèlement contreviennent autant aux règles de droit privé sur la protection de la personnalité (cf. art. 28 ss CC et art. 328 CO) qu'aux règles de droit public sur la protection de la santé (cf. art. 6 LTr ; art. 2 OLT 3)[93].

Le mobbing peut prendre des formes diverses selon le critère des personnes qu'il met en relation : une seule personne peut en harceler une autre ; un groupe de personnes peut participer au harcèlement d'une seule personne ; enfin, un seul employé peut harceler plusieurs personnes lorsqu'il se trouve dans une situation suffisamment influente pour avoir une action sur la situation professionnelle des victimes[94].

Le mobbing peut aussi consister en un « harcèlement administratif ». Le Tribunal fédéral a validé cette notion dans le cas d'un travailleur qui a été harcelé non pas durant la période où il travaillait effectivement, mais lors d'une période pendant laquelle il se trouvait en incapacité de travail. Le harcèlement a consisté dans la multiplication des dé-

88 HOLENSTEIN, p. 45.
89 Voir notamment les études de DEVEAUX-PLÉDRAN et de WENNUBST.
90 Voir, par exemple, TF 4A_245/2009 du 6 avril 2010, consid. 4.2.
91 TF 4A_245/2009 du 6 avril 2010, consid. 4.2 ; TF 4C.343/2003 du 13 octobre 2004, consid. 3.1.
92 Tribunal cantonal vaudois du 25 avril 2001, in : RSJ 98 (2002) 447 ; Tribunal cantonal valaisan du 6 juillet 1998, consid. 3b/aa, in : RVJ 2000 177.
93 DUNAND, Commentaire, N 31 ad art. 328 CO, p. 281.
94 DEVEAUD-PLÉDRAN, p. 24 ; WENNUBST, p. 29 ss.

marches que l'employé a dû entreprendre, face à l'attitude hostile de l'employeur, pour faire reconnaître ses droits et obtenir ses salaires, puis les indemnités versées par l'assurance, ainsi que dans les nombreux courriers et appels téléphoniques que le travailleur a reçus à son domicile pour régler des affaires professionnelles[95]. Il est donc possible qu'un harcèlement administratif soit réalisé par l'envoi renouvelé de courriels intempestifs dans le but d'importuner la victime.

On trouve dans la jurisprudence administrative fédérale un cas de harcèlement psychologique perpétré en partie au moyen d'Internet. Ainsi, dans une décision du 10 mai 2001, la Commission fédérale de recours en matière de personnel fédéral a admis qu'un employé des Chemins de fer fédéraux avait été harcelé psychologiquement pendant plusieurs années par ses collègues de travail, sous la forme notamment d'atteintes à sa faculté d'expression et à sa réputation sociale. Malheureusement, l'état de faits n'a pas été exposé de manière très claire ; on peut toutefois en déduire que la victime avait été obligée lors d'un cours informatique à saisir dans une banque de données des articles tirés d'un catalogue pornographique et on l'avait par la suite dénigrée par la messagerie électronique[96].

2. Harcèlement sexuel

Le harcèlement sexuel sur le lieu de travail constitue non seulement une atteinte grave à la personnalité des travailleurs, au sens de l'article 328 CO, mais aussi une forme grave de discrimination fondée sur le sexe, qui est prohibée par la Loi sur l'égalité. Selon l'article 4 LEg, le harcèlement sexuel comprend « tout comportement importun de caractère sexuel ou tout autre comportement fondé sur l'appartenance sexuelle, qui porte atteinte à la dignité de la personne sur son lieu de travail, en particulier le fait de proférer des menaces, de promettre des avantages, d'imposer des contraintes ou d'exercer des pressions de toute nature sur une personne en vue d'obtenir d'elle des faveurs de nature sexuelle ». On admet cependant que cette définition légale est trop étroite. Ainsi, bien que les exemples cités à l'art. 4 LEg ne se réfèrent qu'à des cas d'abus d'autorité, la loi vise également d'autres types d'actes qui portent atteinte à la dignité du travailleur et qui contribuent à rendre le climat de travail hostile[97].

Selon le Tribunal fédéral, des remarques sexistes, des commentaires grossiers, des plaisanteries déplacées, l'envoi de courriels contenant des caricatures ou des plaisanteries

---

95 TF 4C.74/2007 du 22 janvier 2008, consid. 5.

96 Décision de la Commission fédérale de recours en matière de personnel fédéral du 10 mai 2001, cause PRK 2000-056, in : JAAC 65.96.

97 LEMPEN, N 7 et 8 ad art. 4 LEg, p. 102 s. ; STREIFF/VON KAENEL/RUDOLPH, N 5 ad art. 328 CO, p. 511.

lourdes, à caractère sexuel, ou encore l'affichage d'icônes et de photos indécentes rentrent, par exemple, dans la définition du harcèlement sexuel[98]. Il a été jugé, par exemple, que les trois courriels suivants revêtaient un caractère sexiste suffisant pour importuner la femme qui les avait reçus : le premier contenait une citation de Flaubert selon laquelle « Les femmes des uns font le bonheur des autres » ; le deuxième était une sentence proclamant : « Ne soyez pas méchants avec les femmes … La nature s'en charge au fur et à mesure que le temps passe » ; le troisième contenait un dessin de presse représentant un chef du personnel sur le point de profiter sans scrupule de sa fonction pour regarder sous la minijupe d'une jeune employée en la faisant asseoir en face de son bureau sur une chaise exagérément surélevée[99].

L'existence d'un harcèlement sexuel présuppose que les comportements répréhensibles soient importuns c'est-à-dire non désirés. Selon le Tribunal fédéral, on ne saurait admettre trop facilement l'existence d'un consentement, même tacite, de la personne harcelée. Il s'agissait d'une affaire dans laquelle il avait été constaté un ensemble d'actes constitutifs d'un harcèlement sexuel. Ainsi, des histoires osées circulaient parmi le personnel de la société. Par ailleurs, le directeur s'était une fois exclamé « toutes des salopes » en entrant au secrétariat et il avait demandé à la victime du harcèlement, en présence d'une nouvelle employée, si elle était lesbienne. Un autre collaborateur s'était également adressé à elle de manière grivoise. L'employeur invoquait cependant le consentement de l'employée harcelée : celle-ci aurait échangé sur le système informatique de l'entreprise divers messages personnels contenant des réflexions vulgaires, aurait associé de jeunes collaboratrices à la création de propos honteux sur le réseau informatique, aurait émis régulièrement des remarques et allusions sexuelles lors de dialogues avec les collaborateurs, et aurait, enfin, diffusé des supports pornographiques dans la société et utilisé Internet dans ce but. Le Tribunal fédéral a jugé que l'emploi du même vocabulaire entre collègues de travail, « ne saurait justifier l'admission par l'employeur de remarques sexistes, grossières ou embarrassantes, en particulier de la part d'un supérieur hiérarchique, dont le comportement peut déteindre sur celui de ses subordonnés »[100].

98 ATF 126 III 395, consid. 7b/bb ; TF 4C.289/2006 du 5 février 2007, consid. 3.1.

99 TF 4A_178/2010 du 14 mai 2010, consid. 4.2. Les juridictions ont cependant rejeté la demande en indemnité de la victime en considérant que l'employeur pouvait se prévaloir de la preuve libératoire prévue à l'art. 5 al. 3 LEg (voir consid. 4.3).

100 TF 4C.463/1999 du 4 juillet 2000, consid. 7d.

D. Protection des données

L'article 328 CO qui énonce le régime général de la protection de la personnalité est complété par l'art. 328*b* CO qui contient des règles spécifiques relatives au traitement de données personnelles du travailleur. Selon l'art. 328*b* 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 »[101]. La disposition renvoie pour le surplus à l'application de la Loi fédérale sur la protection des données (LPD).

Les rapports de travail donnent lieu à la collecte et au traitement de nombreuses données personnelles du travailleur et pendant une longue durée[102]. Les données ainsi traitées peuvent constituer des données sensibles (cf. art. 3 let. c LPD) ou des profils de personnalité (cf. art. 3 let. d LPD)[103]. En sa qualité de maître du fichier, l'employeur doit protéger les données personnelles contre tout traitement non autorisé (cf. art. 7 LPD). Les développements technologiques et l'utilisation généralisée de l'ordinateur permet un traitement de données dense, rapide, complexe et globalisé[104]. Par ailleurs, les opérations informatiques laissent des traces qui permettent de procéder à des contrôles détaillés sans que l'utilisateur ne s'en aperçoive[105]. Enfin, l'employé qui utilise un smartphone que lui a remis son employeur peut être facilement géolocalisé (au moyen, par exemple, de l'application MapMyMobile). Le risque d'atteinte importante à la personnalité des travailleurs est manifeste.

Nous traiterons ici de deux questions sensibles, la levée du courrier électronique (sous-section 1) et la cybersurveillance (sous-section 2)[106].

1. Levée du courrier électronique

La gestion du flux de courriels est une question délicate. Meier relève que l'employeur est en droit de sauvegarder globalement l'intégralité des courriels entrants et sortants, qu'ils soient de nature professionnelle ou privée, car il peut se prévaloir d'un intérêt

101 Pour une analyse détaillée de cette disposition légale, cf. DUNAND, Commentaire, ad art. 328*b* CO, p. 317 ss ; FLUECKIGER, p. 97 ss et MEIER, p. 649 ss.

102 MEIER, N 2020, p. 646.

103 COSTA, N 2.

104 MEIER, N 10, p. 62.

105 ORDOLLI, N 6, p. 24.

106 Sur la question de la protection des données dans le cadre de l'utilisation des moyens informatiques, cf. COTTIER, p. 83 ss, ainsi que les contributions dans le présent ouvrage de CHRISTIAN FLUECKIGER (p. 73 ss) et de SYLVAIN MÉTILLE (p. 101 ss).

privé prépondérant, au sens de l'article 13 alinéa 1 LPD, à ne pas devoir faire le tri manuel de ces courriels[107]. Il peut aussi procéder au scannage systématique des courriels dans un but de sécurité et d'efficience[108]. Dans toutes ces opérations, l'employeur prendra garde de ne pas porter atteinte aux droits de la personnalité de ses employés.

Il peut arriver que le travailleur soit absent du lieu de travail pendant plusieurs jours (maladie, vacances, service militaire, etc.) et qu'il ne soit pas en mesure de prendre connaissance du courriel adressé sur son adresse professionnelle. Il existera alors un conflit d'intérêt entre le respect de la sphère privée de l'employé et la bonne marche du service[109]. Le régime juridique dépendra notamment de savoir si le travailleur était autorisé ou non à faire une utilisation privée de la messagerie de l'entreprise. Lorsque l'employeur a interdit l'utilisation de la messagerie à des fins privées, tout message reçu ou envoyé sur la boîte électronique professionnelle de l'employé est présumé appartenir à la sphère de l'employeur[110]. L'accès à la messagerie de l'employé absent sera donc autorisé[111]. Le Préposé fédéral à la protection des données suggère que l'employé désigne un suppléant qui aura le droit de lire et, si nécessaire, de traiter les courriers professionnels entrants[112]. L'employeur devra toutefois traiter les données avec précaution et s'abstenir, dans la mesure du possible, de prendre connaissance du contenu d'un message ou de toute information d'ordre privé[113].

En revanche, lorsque l'employeur a autorisé ou toléré l'utilisation de la messagerie professionnelle à des fins privées, il lui est en principe prohibé d'accéder aux messages reçus par l'employé absent. Il est alors judicieux d'installer un message automatique de réponse prédéfini indiquant à l'expéditeur que le destinataire de l'envoi est absent et qu'il peut contacter au besoin un collègue déterminé. Tout autre moyen, qu'il s'agisse d'une déviation vers la boîte d'un suppléant ou de l'octroi au suppléant d'un droit de consultation de la messagerie de l'absent, comprend un risque élevé de lecture de courriers privés, et par voie de conséquence de violation des règles sur la protection de la personnalité du travailleur absent[114].

Lorsqu'un employé quitte définitivement l'entreprise, son compte de courrier électronique doit être désactivé le dernier jour de travail et sa boîte de messagerie effacée[115]. Il

---

107 MEIER, N 2039, p. 651 s. et N 2187, p. 707.
108 MEIER, N 2194, p. 709.
109 COTTIER, p. 105.
110 CARRUZZO, N 23 ad art. 328*b* CO, p. 343.
111 COTTIER, p. 106.
112 PFPDT, p. 16.
113 MEIER, N 2176, p. 703.
114 COTTIER, p. 106.
115 PFPDT, p. 17.

faut cependant tenir compte du fait que l'employeur a l'obligation de conserver certaines données après la fin du contrat de travail, car leur traitement concerne l'exécution du contrat ou sont justifiées par d'autres obligations légales de l'employeur[116]. Par exemple, les entreprises soumises à l'obligation de tenir une comptabilité doivent conserver pendant dix ans les livres et les pièces comptables (cf. art. 958*f* CO). Cela peut aussi concerner des données contenues dans des courriers électroniques (voir également les dispositions de l'Ordonnance concernant la tenue et la conservation des livres de compte (Olico) du 24 avril 2002[117])[118].

Sous réserve de ce qui précède, lorsqu'un usage privé de la messagerie a été expressément interdit, l'employeur est en droit de consulter, d'archiver ou de détruire librement les courriels figurant dans la messagerie professionnelle utilisée par l'employé quittant l'entreprise, pour autant qu'il s'abstienne de prendre connaissance du contenu de messages privés que la boîte contiendrait. En revanche, lorsqu'un usage privé a été autorisé ou toléré, l'employeur n'a aucun droit d'accéder aux messages privés[119]. Il doit, en conséquence, offrir au travailleur la possibilité de les récupérer sur un support privé, puis les faire effacer des serveurs de l'entreprise[120].

2. Cybersurveillance

L'utilisation d'Internet et du courrier électronique laisse de nombreuses traces. Les fichiers journaux des activités exécutées, permettant le contrôle des activités des employés, peuvent notamment se trouver sur le poste de travail de l'utilisateur, sur les serveurs Intranet ou encore sur les équipements de connexion inter-réseaux (pare-feux ou routeurs)[121]. C'est dire que la cybersurveillance est techniquement facile et discrète puisqu'elle peut s'opérer rapidement et en toute discrétion sans que l'utilisateur ne soit au courant.

Le contrôle de l'utilisation de la messagerie et d'Internet par les employés n'est pas illicite en soi[122]. L'employeur a, en effet, le droit de vérifier la correcte exécution de la prestation de travail et de s'assurer que les ressources informatiques sont utilisées conformément aux normes légales. Il peut également s'assurer que l'intégrité, la fiabilité et

116 DUNAND, Commentaire, N 102 ad art. 328*b* CO, p. 348.
117 RS 221.431.
118 ALDER, p. 276 s.
119 Jugement du Tribunal des prud'hommes de Zurich du 10 décembre 2003, in : JAR 2004, p. 606 ; Jugement du Tribunal arbitral des prud'hommes de Bâle-Ville du 29 janvier 2001, in : JAR 2004, p. 440.
120 CARRUZZO, N 23 ad art. 328*b* CO, p. 343 ; PFPDT, p. 17.
121 PFPDT, p. 5.
122 COTTIER, p. 96 ; BRUNNER/BÜHLER/WAEBER/BRUCHEZ, N 5 ad art. 328 CO, p. 143

la sécurité des données sont bien respectées[123]. Pour être licite, la surveillance doit respecter les principes applicables en matière de traitement des données, ainsi que les prescriptions de la législation sur le travail (notamment l'art. 26 OLT 3)[124]. De plus, des précautions particulières doivent être prises quant à l'étendue et aux modalités de la surveillance[125].

Lorsqu'il a interdit toute utilisation à des fins privées, l'employeur a en principe un droit de contrôle étendu sur l'utilisation de la messagerie de l'entreprise[126]. Il peut notamment vérifier les destinataires et les expéditeurs, ainsi que l'objet indiqué en rubrique des courriels transitant par la boîte professionnelle[127]. Il s'abstiendra cependant, dans la mesure du possible, de prendre connaissance du contenu d'un message privé qui aurait transité sur la messagerie professionnelle[128]. Il devra encore moins consulter des envois qui transiteraient par une boîte privée[129]. En revanche, lorsqu'il a autorisé ou toléré une utilisation privée, le droit de contrôle est plus limité[130]. En particulier, l'employeur ne doit pas avoir accès aux courriels privés des employés[131].

Dans son Guide relatif à la surveillance de l'utilisation d'Internet et du courrier électronique au lieu de travail, le Préposé fédéral à la protection des données et à la transparence propose une marche à suivre[132] qui a été validée récemment par le Tribunal fédéral[133] et largement codifiée par le Parlement pour l'administration fédérale[134]. A titre préalable, le Préposé fédéral conseille à l'employeur, d'une part, d'édicter des directives sur l'utilisation et la surveillance des moyens de communication électronique, et d'autre

123 MEIER, N 2156, p. 697.

124 ATF 139 II 7, consid. 5, JdT 2013 II 188 (rés.), SJ 2013 I 177 (rés.). Sur ces questions, voir également COSTA ; DUNAND, Commentaire, N 85 ss ad art. 328*b* CO, p. 342 ss ; MEIER, p. 685 ss, PFPDT, p. 6 ss, ainsi que la contribution de SYLVAIN MÉTILLE dans le présent ouvrage, p. 99 ss.

125 COTTIER, p. 96 ss.

126 MEIER, N 2173, p. 702 ; STREIFF/VON KAENEL/RUDOLPH, N 18 ad art. 328*b* CO, p. 622.

127 MEIER, N 2176, p. 703.

128 STREIFF/VON KAENEL/RUDOLPH, N 18 ad art. 328*b* CO, p. 622.

129 COTTIER, p. 100.

130 VON KAENEL, Internet, p. 44 s.

131 COTTIER, p. 100.

132 PFPDT, p. 8 ss. Sur ces questions, voir les développements de HOLENSTEIN, p. 110 ss.

133 ATF 139 II 7, consid. 5.5, JdT 2013 II 188 (rés.), SJ 2013 I 177 (rés.). Notre Haute Cour considère que le Guide du Préposé constitue une aide interprétative importante de l'art. 26 OLT 3 et qu'il peut être considéré comme assurant un standard minimum pour la surveillance informatique (consid. 5.5.1).

134 Cf. les art. 57*i* à 57*q* de la Loi sur l'organisation du gouvernement et de l'administration (LOGA) du 21 mars 1997, RS 172.010.

part, de prendre des mesures techniques de prévention (blocage de certains sites, installation d'antivirus, etc.), qui permettront d'éviter la majorité des problèmes potentiels[135].

Il est tout d'abord possible de procéder, sans information préalable à la journalisation de la navigation des collaborateurs sur Internet[136]. Par ailleurs, en cas de dérangement technique, le responsable de la sécurité informatique doit se voir reconnaître le droit de dépouiller immédiatement les fichiers informatiques concernés[137]. S'agissant des modalités de contrôle, elles doivent respecter le principe de la proportionnalité[138]. On distingue trois formes d'analyse : anonyme, pseudonyme et nominale. L'employeur peut procéder librement, sans information préalable, à des contrôles globaux, permanents et anonymisés (qui ne se rapportent pas aux personnes) portant sur l'analyse statistique des fichiers journaux[139]. En revanche, il ne devrait recourir à des contrôles pseudonymisés (analyses non nominales se rapportant aux personnes) que si la mesure a fait l'objet d'une information préalable ou si elle est mentionnée dans le règlement[140]. Les analyses pseudonymes peuvent être effectuées même en l'absence d'un soupçon concret d'abus[141]. Enfin, il ne sera procédé à une analyse nominale que dans le cas où des abus ont été constatés, c'est-à-dire lorsqu'un employé paraît avoir enfreint les dispositions de la loi ou d'un règlement d'utilisation[142]. En principe, aucun contrôle nominatif ne devrait être ordonné sans information préalable des employés, que celle-ci ait été donnée peu avant le déclenchement d'une opération ou au moins antérieurement par la communication d'un règlement d'utilisation[143]. Les contrôles ciblés devront être ponctuels, limités dans le temps[144] et les données seront protégées de tout accès indu[145]. Une fois le contrôle effectué, le travailleur concerné sera personnellement informé de la mesure et des résultats de la surveillance[146]. Le travailleur bénéficie en principe d'un droit d'accès à toutes les données le concernant qui sont contenues dans le fichier, y compris les informations disponibles sur l'origine des données (cf. art. 8 LPD)[147].

135 PFPDT, p. 8 ss.
136 MEIER, N 2210, p. 714.
137 WYLER, p. 307 s.
138 MEIER, p. 713 ss.
139 MEIER, N 2210, p. 714 ; PFPDT, p. 10.
140 MEIER, N 2210, p. 714 s.
141 PFPDT, p. 10.
142 BRUNNER/BÜHLER/WAEBER/BRUCHEZ, N 5 ad art. 328 CO, p. 143 ; COTTIER, p. 98 ; MEIER, N 2210, p. 715.
143 COTTIER, p. 103 ss ; MEIER, N 2207, p. 712 s.
144 COTTIER, p. 102.
145 MEIER, N 2212, p. 716.
146 COTTIER, p. 101.
147 PFPDT, p. 11.

Comme l'a jugé récemment le Tribunal fédéral, il est en principe interdit de procéder à une surveillance permanente au moyen d'espiologiciels (*spywares*), susceptibles d'enregistrer l'ensemble des activités produites sur l'ordinateur[148]. En revanche, lorsqu'il soupçonne de manière fondée un employé d'avoir commis ou de s'apprêter à commettre une infraction pénale ou de porter gravement atteinte aux intérêts de l'entreprise, l'employeur est en droit de procéder à une surveillance nominative, même sans information préalable, dans la mesure où il peut se prévaloir d'un intérêt privé prépondérant voire d'un intérêt public[149]. L'accès au contenu de courriels est par exemple licite lorsque l'employé a utilisé les moyens de communication de l'entreprise pour commettre des infractions pénales ou des actes déloyaux à l'encontre de son employeur[150].

E. Responsabilité de l'employeur

En cas d'atteinte à la santé ou à la personnalité de ses employés sur le lieu de travail, l'employeur est susceptible d'être actionné sur les plans administratif, civil et pénal[151].

Lorsque l'employeur contrevient aux prescriptions de la législation sur le travail, par exemple les dispositions sur la durée du travail et du repos (art. 9 ss LTr), il encourt des sanctions administratives et pénales. Dans la règle, un avertissement assorti d'un délai raisonnable est donné à l'employeur afin qu'il prenne les mesures adéquates (art. 51 al. 1 LTr). S'il ne donne pas suite à cette intervention, l'autorité cantonale prendra la décision voulue, sous la menace de la peine prévue à l'article 292 du Code pénal suisse (art. 51 al. 2 LTr)[152]. L'article 59 régit la responsabilité pénale de l'employeur. Est ainsi punissable l'employeur qui enfreint les prescriptions sur la protection de la santé, qu'il agisse intentionnellement ou par négligence (art. 59 al. 1 let. a LTr), ou qui enfreint les prescriptions sur la durée du travail ou du repos, s'il agit intentionnellement (art. 59 al. 1 let. b LTr). En principe, la contrainte pénale présente un caractère subsidiaire par rapport à la contrainte administrative. Suivant les circonstances, l'autorité cantonale compétente peut cependant suivre les deux voies en parallèle, voire recourir à la voie pénale seule, si les mesures administratives se révélaient d'emblée être inopérantes[153].

---

148 ATF 139 II 7, consid. 5, JdT 2013 II 188 (rés.), SJ 2013 I 177 (rés.). Voir également MEIER, N 2213, p. 717.

149 TF 9C_785/2010 du 10 juin 2011, consid. 6.7.3 ; MEIER N 2152, p. 695 et N 2211, p. 716 s.

150 MEIER, N 2189, p. 707.

151 Sur ces questions, voir SONNENBERG, ainsi que les contributions parues in : KAHIL-WOLFF/WYLER.

152 TF 2P.207/2002 du 20 juin 2003, consid. 1.1.2.

153 TF 2A.423/2000 du 22 mars 2001, consid. 2a.

Sur le plan civil, l'employeur qui exige une disponibilité continue et ne respecte pas les règles applicables en matière de vacances, de congés ou d'heures de repos s'expose à devoir rétribuer et/ou compenser les heures de travail effectuées en trop. Plus généralement, l'employé atteint dans ses droits de la personnalité, du fait par exemple d'un harcèlement psychologique ou d'une mesure de surveillance illicite, pourra se prévaloir des actions prévues dans le Code civil (cf. art. 28*a* CC), et actionner l'employeur en dommages-intérêts (art. 97 ss CO), en réparation du tort moral (art. 49 CO) ou en versement de l'indemnité prévue dans la Loi sur l'égalité en cas de harcèlement sexuel (art. 5 al. 3 et 4 LEg)[154]. Une atteinte aux droits de la personnalité du travailleur constitue autant un acte illicite, susceptible d'engager la responsabilité délictuelle de l'employeur (cf. art. 41 al. 1 CO) qu'une violation du contrat de travail, susceptible d'engager sa responsabilité contractuelle (cf. art. 97 al. 1 et 328 CO). On rappellera que l'employeur répond de ses propres actes, y compris ceux de ses organes (cf. art. 55 al. 2 CC), ainsi que des actes de ses auxiliaires (cf. art. 55 et 101 CO)[155]. Il devra, par exemple, répondre des actes de harcèlement psychologique sur l'un de ses employés, perpétrés au moyen de courriels inappropriés adressés par des collègues de travail.

Le travailleur qui subit un dommage matériel ou une atteinte à la santé découlant d'une atteinte illicite à ses droits de la personnalité a droit à une réparation sous forme de dommages-intérêts[156]. Il devra prouver le dommage, la violation contractuelle, ainsi que le lien de causalité entre les deux. En revanche, la faute de l'employeur est présumée. Le travailleur pourra aussi prétendre au paiement d'une indemnité pour tort moral, pour autant que la gravité de l'atteinte le justifie et que l'employeur ne lui ait pas donné satisfaction autrement (cf. art. 49 CO)[157]. Un employeur a, par exemple, été condamné à verser une somme de 1'000 frs. à titre de réparation morale à une employée dont il avait, en son absence et sans l'avertir, ouvert et lu plusieurs courriels de nature privée, et pris connaissance de la liste des sites web qu'elle avait consultés[158]. Toutefois, dans un arrêt récent, le Tribunal fédéral a précisé qu'il ne suffisait pas pour obtenir une réparation morale que la victime démontre avoir fait l'objet d'une atteinte à sa sphère privée, en l'occurrence parce que l'employeur avait accédé à sa messagerie privée. Il fallait encore alléguer et prouver les faits permettant de constater que l'atteinte était objectivement et subjectivement grave[159].

---

154 BRUNNER/BÜHLER/WAEBER/BRUCHEZ, N 15 et 16 ad art. 328 CO, p. 149 s. ; DUNAND, Commentaire, N 64 ss ad art. 328 CO, p. 293 ss.

155 DUNAND, Commentaire, N 10 ad art. 328 CO, p. 273 et N 88 ss ad art. 328 CO, p. 304 ss.

156 DUNAND, Commentaire, N 79 ss ad art. 328 CO, p. 298 s.

157 DUNAND, Commentaire, N 83 ss ad art. 328 CO, p. 299 ss.

158 Jugement du Tribunal des prud'hommes de Zurich du 10 décembre 2003, in : JAR 2004, p. 606.

159 TF 4A_465/2012 du 10 décembre 2012, consid. 3.2.

En cas de harcèlement sexuel, le tribunal pourra en principe condamner l'employeur à verser à la victime une indemnité fixée compte tenu de toutes les circonstances et qui doit être calculée sur la base du salaire moyen suisse (art. 5 al. 3 LEg). L'indemnité ne peut excéder le montant correspondant à six mois de salaire de la victime (art. 5 al. 4 LEg). La loi institue toutefois une preuve libératoire en faveur de l'employeur qui parvient à prouver qu'il a pris les mesures que l'expérience commande, qui sont appropriées aux circonstances et que l'on peut équitablement exiger de lui pour prévenir le harcèlement sexuel ou y mettre fin (art. 5 al. 3 LEg)[160]. Ainsi, la victime de courriels à caractère sexiste ne peut recevoir l'indemnité prévue en cas de harcèlement sexuel si l'employeur peut se prévaloir de la preuve libératoire en prouvant qu'il a pris les mesures utiles pour faire cesser la diffusion de courriels contrevenants à la LEg[161].

Enfin, lorsqu'il a été surveillé de manière illicite, l'employé pourra également engager une poursuite pénale contre l'employeur, par exemple pour violation du domaine secret ou du domaine privé au moyen d'un appareil de prises de vues (art. 179^{quater} CP), ou pour soustraction de données personnelles (art. 179^{novies} CP)[162].

IV. Règlement d'utilisation

Il résulte des considérations qui précèdent qu'il est hautement recommandé aux entreprises d'édicter des directives ou un règlement d'utilisation et de surveillance des moyens informatiques[163]. Formellement, le règlement doit être clairement communiqué et expliqué (section A). Matériellement, le règlement précisera les droits et les obligations des employés (section B), fixera les mesures de surveillance (section C) et règlera les sanctions des éventuels abus (section D). Il est conseillé de compléter le dispositif par des mesures techniques préventives (section E).

A. Communication du règlement

Pour être efficace, le règlement doit être communiqué clairement, expliqué et compris par les employés. Il est conseillé d'en transmettre une copie à chaque travailleur et de lui demander d'en accuser réception par sa signature apposée sur un document gardé en possession de l'employeur. Lorsque les règlements sont publiés en ligne, il est indiqué

160 Cf. LEMPEN, p. 113 ss.
161 TF 4A_178/2010 du 14 mai 2010, consid. 4.3.
162 PFPDT, p. 17 ; VON KAENEL, Internet, p. 45 ss.
163 Notons que le PFPDT propose un règlement type, p. 13 ss.

d'adresser aux employés un courriel électronique contenant le lien qui mène au règlement[164]. Il peut être utile aussi d'organiser régulièrement des séances d'information ou de sensibilisation. Dans certaines entreprises, il est demandé chaque année aux collaborateurs de lire une nouvelle fois les divers règlements et de confirmer par leur signature qu'ils en ont compris et accepté le contenu[165]. C'est à l'employeur de prouver la communication effective et le contenu des directives et instructions[166]. L'employeur doit évidemment informer les employés de toute modification du règlement.

L'employeur peut aussi envisager de consulter les employés avant d'édicter le règlement. Une démarche participative est de nature à favoriser l'adhésion des employés aux finalités du règlement. La Loi sur le travail prévoit une obligation d'information et de consultation des travailleurs ou de leurs représentants dans l'entreprise lorsqu'il s'agit notamment de questions relatives à la sécurité au travail (cf. art. 48 LTr).

L'application d'un règlement peut devenir inopérante si l'employeur n'en contrôle pas le respect[167]. En effet, lorsqu'il tolère des violations répétées, les employés peuvent présumer qu'il a renoncé à s'en prévaloir. L'employeur court aussi le risque du manque de précision du règlement. Le Tribunal fédéral a, par exemple, considéré que le fait d'adresser des messages électroniques avec un contenu pornographique à des personnes consentantes ne pouvait être considéré comme une violation des directives de l'entreprise qui ne prohibaient expressément que les comportements constitutifs d'un harcèlement sexuel[168]. Enfin, lorsque l'employeur reprend des modèles internationaux ou étrangers, par exemple dans le cadre d'une société multinationale, il vérifiera leur conformité au droit suisse[169].

B. Droits et obligations des employés

Le premier but du règlement est de préciser les droits et les obligations des employés. Chaque règlement doit être adapté aux besoins et à la philosophie de l'entreprise. Il pourra, dans cette optique, être plus ou moins précis et détaillé. Il contiendra généralement des règles sur :

– l'objet et les buts du règlement ;
– l'utilisation, l'accès, les mots de passe, le stockage et l'archivage des données ;

164 PFPDT, p. 9.
165 PASCHE, p. 71.
166 DUNAND, Commentaire, N 12 ad art. 321*d* CO, p. 108.
167 SUBILIA, p. 56 s.
168 TF 4C.109/2003 du 30 juillet 2003, consid. 2.2.2-3.
169 MEIER, N 2209, p. 713.

- les mesures prises en cas d'absence prolongée d'un collaborateur ;
- la sécurité du réseau et des serveurs ;
- l'utilisation d'Internet, de la messagerie, des imprimantes et des photocopieuses en réseau ;
- les mesures de contrôle et de surveillance ;
- les sanctions.

Il est, tout d'abord, impératif d'établir quelques règles générales et essentielles, appelées parfois « bonnes pratiques » ou « règles d'or », précisant que l'utilisation des moyens informatiques :

- doit être conforme à la loi, aux conventions collectives de travail, aux contrats-types de travail, aux règlements et directives d'utilisation, ainsi qu'aux instructions reçues ;
- doit être conforme à l'obligation de diligence et de fidélité (cf. art. 321*a* CO) ;
- doit respecter les règles sur la sécurité et la confidentialité des données ;
- ne doit pas porter atteinte à la personnalité ou à la santé des collègues de travail (cf. art. 328 CO ; art. 6 LTr).

Il convient aussi de régler les modalités d'une utilisation à des fins privées d'Internet et de la messagerie électronique, pendant ou en dehors des heures de travail, dans les locaux ou à l'extérieur de l'entreprise. L'utilisation privée doit être compatible avec l'obligation de consacrer tout son temps de travail à son employeur (art. 319 et art. 321*d* CO). Celui-ci peut imposer, par exemple, qu'elle s'effectue :

- de manière occasionnelle et raisonnable, dans la mesure où elle ne compromet pas l'activité professionnelle ;
- et/ou pendant les pauses ou en dehors des heures de travail (par exemple, « entre 12h00 et 13h00 » ou « après 18h00 ») ;

Enfin, suivant le degré de précision souhaité, le règlement contiendra des règles sur l'interdiction d'utilisations et de comportements considérés comme répréhensibles ou inopportuns, tels que :

- la communication du mot de passe personnel à un collègue ou un tiers ;
- l'utilisation de systèmes de messageries personnelles à travers des services de messagerie non officiels (par exemple, hotmail) ;
- la création de sites ou de pages à des fins non professionnelles ;
- le téléchargement ou l'installation de logiciels ;
- le transfert de courrier électronique ou de fichiers à caractère professionnel à son adresse privée ;

- l'envoi de masse à des fins privées, la propagation de messages « chaînés » et de fausses rumeurs (hoax) ;
- l'accès à certains sites figurant sur une liste négative ;
- l'accès à des sites payants ;
- l'accès à des forums de discussion ;
- la participation aux réseaux sociaux ;
- la communication d'informations et de critiques portant sur les dirigeants ou la stratégie de l'entreprise ;
- l'envoi de fichiers ou la visite de sites à caractère érotique ;
- l'utilisation dans un but lucratif ou de publicité privée ;
- l'utilisation aux fins de transactions financières, notamment le « telebanking ».

C. Mesures de surveillance

Le deuxième but d'un règlement est de préciser les conditions et les modalités des mesures de surveillance. Comme nous l'avons déjà précisé, cela permettra notamment à l'employeur de procéder à des contrôles pseudonymisés ou des contrôles nominatifs sans avoir à donner une information spécifique individuelle à chaque fois[170].

Le règlement devrait indiquer que l'employeur est en droit de procéder à :

- la journalisation de la navigation des collaboratrices et collaborateurs de l'entreprise ;
- des contrôles anonymisés ;
- des contrôles pseudonymisés ;
- des contrôles nominatifs en cas de soupçons d'utilisation abusive par des personnes déterminées.

Le règlement contiendra également des dispositions sur les modalités de la surveillance quant à ses finalités, aux catégories de données enregistrées, à la durée de conservation et aux personnes ayant accès aux données[171].

170 MEIER, N 2207, p. 712 s.
171 MEIER, N 2210, p. 715.

D. Sanction des abus

Le troisième but d'un règlement est d'annoncer les sanctions qui seront prises envers les employés qui ne respectent pas les obligations prévues dans la loi, le règlement d'utilisation et le contrat. Ces clauses seront utiles pour rendre les employés attentifs à l'importance pour l'employeur du respect de leurs devoirs. La mention de sanctions dans un règlement ne les rend toutefois pas immédiatement opérationnelles. Tout d'abord, bien qu'il soit techniquement facile d'établir une violation du règlement puisque tout utilisateur de moyens informatiques doit s'identifier et laisse nécessairement des traces de ses activités, la possibilité pour l'employeur d'établir la preuve des manquements ne va pas de soi[172]. Il faut tenir compte du fait qu'une preuve obtenue de manière illégale, notamment parce qu'elle résulte d'une surveillance illicite, pourra être écartée par les tribunaux[173]. Par ailleurs, une sanction ne pourra être appliquée dans un cas d'espèce que dans les limites tracées par la loi et la jurisprudence. Enfin, lorsque l'employeur ne met pas rapidement en œuvre la sanction après la découverte du manquement, il risque de se voir opposer une renonciation tacite à s'en prévaloir[174].

Les règlements reprennent parfois le texte de certaines dispositions sur le contrat de travail (par exemple, de l'article 321*a* CO sur l'obligation de diligence et de fidélité, ou de l'article 337 CO sur les justes motifs en cas de résiliation immédiate) pour en souligner la portée. Il est également possible de prévoir des sanctions complémentaires (par exemple, une clause pénale au sens des art. 160 ss CO).

Il est possible, par exemple, de prévoir que tout manquement grave sera sanctionné par un licenciement immédiat. En cas de litige, l'employeur devra toutefois prouver l'existence des conditions matérielles et formelles requises (justes motifs, avertissements, immédiateté, respect des formes convenues) pour la bonne application de l'article 337 CO[175]. Or, comme nous l'avons vu, la jurisprudence a souvent considéré, dans des litiges portant sur une utilisation abusive des moyens informatiques, que la résiliation immédiate du contrat de travail était injustifiée. Dans la plupart des cas, et malgré une clause contenue dans le règlement d'utilisation, l'employeur devra donc notifier un ou plusieurs avertissements avant de résilier le contrat de manière immédiate[176].

---

172 Cf. SUBILIA, p. 60 ss.

173 Cf. ATF 139 II 7, consid. 6, JdT 2013 II 188 (rés.), SJ 2013 I 177 (rés.), ainsi que la contribution de SYLVAIN MÉTILLE dans le présent ouvrage (p. 123 ss).

174 CARRUZZO, N 11 ad art. 321*d* CO, p. 90.

175 GLOOR, N 71 ad art. 337 CO, p. 769.

176 GLOOR, N 22 ad art. 337 CO, p. 742 s.

L'employeur supporte le risque de la formulation maladroite d'une clause réglementaire. Dans une affaire tranchée par le Tribunal fédéral, une entreprise avait édicté des règles de bonne conduite qui interdisaient d'effectuer des appels téléphoniques ou d'utiliser la messagerie électronique à des fins privées. Elles précisaient que leur violation était susceptible d'entraîner « une action disciplinaire pouvant aller jusqu'à et y compris le licenciement ». Il nous apparaît que cette dernière clause était inutile voire contre-productive puisqu'en droit suisse prévaut la liberté de résiliation, de sorte que, pour être valable, un congé n'a en principe pas besoin de reposer sur un motif particulier[177]. Dans le cas d'espèce, le Tribunal fédéral, suivant l'avis des juridictions cantonales, a considéré comme injustifiée la résiliation immédiate notifiée à l'employé à qui l'employeur reprochait une utilisation abusive d'Internet et du téléphone de la société. Il est en effet apparu que le travailleur ne pouvait comprendre qu'il serait congédié séance tenante en cas de récidive, « alors que son contrat et le règlement interne de l'entreprise prévoyaient expressément des sanctions moins radicales pour les agissements qui lui étaient reprochés, la plus incisive étant le « licenciement » sans précision aucune au sujet de son éventuel caractère immédiat »[178].

L'employeur peut aussi se réserver la possibilité d'infliger des sanctions disciplinaires (autres que celles prévues dans la loi)[179]. Il n'est toutefois pas admissible de prévoir que le travailleur est soumis au pouvoir disciplinaire général de l'employeur que celui-ci exercerait selon son bon vouloir[180]. En effet, toute sanction doit être proportionnée, déterminée ou déterminable et circonscrite[181]. Pour les entreprises soumises à la législation sur le travail, « des sanctions disciplinaires ne peuvent être infligées qu'au cas et dans la mesure où le règlement d'entreprise le prévoit d'une manière convenable » (art. 38 al. 1 LTr).

L'institution d'une peine conventionnelle sanctionnant un manquement du travailleur est parfaitement possible[182]. Un tel mécanisme est d'ailleurs prévu en cas de violation d'une clause d'interdiction de concurrence (cf. art. 340*b* al. 2 CO). En principe, les parties peuvent fixer librement le montant de la peine (art. 163 al. 1 CO), étant entendu que le juge doit réduire les peines qu'il estime excessives (art. 163 al. 2 CO)[183]. La mise en œuvre de la peine conventionnelle pourra toutefois être délicate, car il faut distinguer la

177 ATF 132 III 115, consid. 2.1, JdT 2006 I 152.
178 TF 4C.173/2003 du 21 octobre 2003, consid. 3.2. Voir aussi, dans la même affaire : TF 4P.133/2003 du 21 octobre 2003, consid. 1.
179 MEIER, N 2208, p. 713.
180 ATF 119 II 162, consid. 2, JdT 1994 I 105.
181 CARRUZZO, N 11 ad art. 321*d* CO, p. 90 ; WYLER, p. 148.
182 SANTORO, p. 41 ss.
183 SANTORO, p. 109 ss.

peine qui constitue une convention d'indemnisation forfaitaire de celle qui institue une simple amende ou clause pénale[184]. Une clause pénale a d'ailleurs elle-même une fonction d'indemnisation et de répression[185]. Or, en droit du travail, lorsque la peine conventionnelle comporte un aspect d'indemnisation, elle ne saurait contourner le régime de la responsabilité contractuelle du travailleur prévu à l'article 321*e* CO et contraindre celui-ci à payer à son employeur une somme supérieure au montant qu'il aurait été tenu de verser, à titre de réparation, selon cette disposition légale[186].

Vu ces difficultés, l'employeur préférera parfois prévoir des sanctions de nature technique, comme la suppression de l'accès à certains sites ou le blocage de l'accès à Internet. En revanche, la violation du devoir de diligence et de fidélité par le travailleur ne peut impliquer en elle-même une réduction – ou a fortiori une suspension – de son salaire, à titre de sanction, car le salaire ne dépend pas d'un résultat ou de la bonne exécution du travail[187]. Demeure réservé le cas de la demeure du travailleur, lorsque celui-ci ne fournit pas sa prestation bien qu'il soit apte au travail[188].

E. Mesures techniques

L'employeur a tout intérêt à recourir à diverses mesures techniques ou organisationnelles qui limiteront les abus ou les risques de l'entreprise[189]. Il s'agit tout d'abord de mettre en place un système rigoureux de gestion des mots de passe, comprenant l'obligation de déconnexion en cas d'absence du poste de travail, et de crypter ou chiffrer les données confidentielles. L'employeur doit protéger le réseau informatique contre tout traitement non autorisé par des mesures organisationnelles qui déterminent les personnes compétentes et des mesures techniques assurant la journalisation des accès aux fichiers journaux[190].

L'employeur prendra garde aussi de faire installer des logiciels antivirus, régulièrement mis à jour, ainsi que des pare-feux (firewalls) permettant de rendre le contenu du réseau interne invisible de l'extérieur. Il est aussi recommandé de mettre en œuvre des gestionnaires de quotas qui permettent de limiter l'espace disque dont peut disposer un utilisa-

184 FARNER, p. 220 ss ; WERRO, p. 2 ss.
185 WERRO, p. 3.
186 AUBERT, N 7 ad art. 321*e* CO, p. 1986 ; SANTORO, p. 46 ss.
187 DUNAND, Commentaire, N 83 ad art. 321*a* CO, p. 75 ; BRUNNER/BÜHLER/WAEBER/BRUCHEZ, N 6 ad art. 321*a* CO, p. 57 ; SUBILIA/DUC, N 9 ad art. 321 CO, p. 116 et N 4 ad art. 321*a* CO, p. 119.
188 CARRUZZO, N 2 ad art. 324*a* CO, p. 195.
189 Sur ces questions, voir HOLENSTEIN, p. 107 ss ; SUBILIA, p. 57 ss.
190 PFPDT, p. 9.

teur pour ses fichiers et courriers électroniques et d'éviter ainsi des surcharges inutiles du réseau[191].

Enfin, il est également possible de bloquer l'accès à certains sites (par exemple des sites pornographiques ou racistes, les réseaux sociaux ou jeux en ligne), l'usage de certains types de fichiers (par exemple photo, vidéo ou audio)[192] ou encore de bloquer tout téléchargement de programmes sur l'ordinateur[193]. Certaines entreprises, rendent impossible de se connecter, à partir des ordinateurs de l'entreprise ou de son réseau, sur des messageries privées auprès desquelles les employés auraient des comptes (par exemple, hotmail ou bluewin)[194].

Pour qu'elles soient efficaces, les mesures préventives doivent être régulièrement adaptées aux développements technologiques et le réseau informatique être configuré en conséquence[195].

V. Conclusion

Les nouvelles technologies ont modifié notre mode de vie, en particulier notre relation à l'information et à la communication. Elles ont également transformé en profondeur l'activité des entreprises et des administrations publiques. Elles ont rendu moins certaines les notions de lieu et de temps de travail et effacé progressivement la distinction entre sphère professionnelle et sphère privée. Sources exponentielles de dynamisme et d'efficacité, elles génèrent aussi des risques incommensurables.

L'usage d'Internet sur le lieu de travail pose de nombreuses questions juridiques qui sont loin d'être résolues. Les développements technologiques sont toujours plus rapides que le droit. Nous avons tenté dans cette contribution d'apporter quelques clarifications sur les droits et obligations de l'employeur et du travailleur. Le juriste peut contribuer à définir les règles d'un usage loyal et conforme au droit des moyens informatiques dans l'entreprise en collaborant notamment à la rédaction de règlements d'utilisation. L'interdisciplinarité est cependant de mise. Le juriste a, en effet, besoin du concours de l'informaticien pour mettre en œuvre les mesures techniques de protection et du spécialiste en gestion des ressources humaines pour optimiser l'utilisation d'Internet par des processus innovants.

---

191 PFPDT, p. 8.
192 COTTIER, p. 97 ; MEIER, N 2199, p. 710.
193 PASCHE, p. 74.
194 PASCHE, p. 74.
195 MONDINI, p. 364.

VI. Bibliographie

ALDER DANIEL, E-Mail-Daten am Arbeitsplatz im Fokus von Datenschutz- und Arbeitsrecht, Revue de l'avocat 6/7/2013, p. 276-279.

AUBERT GABRIEL, Commentaire des art. 319-362 CO, in : THÉVENOZ/WERRO (édit.), Commentaire romand, Code des obligations I, Bâle 2012.

BAUMGARTNER URS, Wenn sich der Datenschützer in das Arbeitsrecht einmischt, PJA 2003, p. 1432-1440.

BIRKHAÜSER/HADORN, BYOD – Bring Your Own Device – Private Smartphones im geschäftlichen Arbeitsumfeld, RSJ 109/2013, p. 201-207.

BRUNNER/BÜHLER/WAEBER/BRUCHEZ, Commentaire du contrat de travail, 3e éd., Lausanne 2004.

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

CEROTTINI ERIC, Commentaire des articles 329 à 329*f* CO, in : DUNAND/MAHON (édit.), Commentaire du contrat de travail, Berne 2013.

COSTA GIORDANO, Internet- und E-Mail-Überwachung am Arbeitsplatz, Jusletter du 9 janvier 2012.

COTTIER BERTIL, La protection des données, in : PERRIN (édit.), Internet au lieu de travail, Lausanne 2004, p. 81-108.

DEVEAUD-PLEDRAN MARIE, Le harcèlement dans les relations de travail, Genève/Zurich/Bâle 2011.

DUNAND JEAN-PHILIPPE, L'usage de l'Internet sur le lieu de travail au vu de la jurisprudence récente du Tribunal fédéral, in : PERRIN (édit.), Internet au lieu de travail, Lausanne 2004, p. 1-35 (cité : DUNAND, L'usage de l'Internet).

DUNAND JEAN-PHILIPPE, Commentaire des articles 321*a*, 321*d*, 321*e*, 328 et 328*b* CO, in : DUNAND/MAHON (édit.), Commentaire du contrat de travail, Berne 2013 (cité : DUNAND, Commentaire).

EGLI URS, Soziale Netzwerke und Arbeitsverhältnis, Jusletter du 17 janvier 2011.

FARNER MARTIN, Die Sicherung der Treuepflicht mit Konventionalstrafe, in : Revue de l'avocat 5/2013, p. 219-223.

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

GEISER THOMAS, Neue Arbeitsformen – Flexible Arbeitsformen, Job Sharing, Computer-Arbeitsplätze, PJA 5/95, p. 557-568 (cité : GEISER, Neue Arbeitsformen).

GEISER THOMAS, Die Beaufsichtigung des Internetbenutzers im Arbeitsrecht, medialex 4/01, p. 201-209 (cité : GEISER, Die Beaufsichtigung).

GLOOR WERNER, Commentaire de l'article 337 CO, in : DUNAND/MAHON (édit.), Commentaire du contrat de travail, Berne 2013.

KAHIL-WOLFF/WYLER (édit.), Assurance sociale, responsabilité de l'employeur, assurance privée, Berne 2005.

HOLENSTEIN CHRISTOPH, Die Benutzung von elektronischen Kommunikationsmitteln (Internet und Intranet) im Arbeitsverhältnis, Berne 2002.

LANGHEINRICH/KARJOTH, Soziale Netzwerke als Risiko für Unternehmen, digma 2010, p. 50-55.

LEMPEN KARINE, Commentaire de l'art. 4 LEg, in : AUBERT/LEMPEN (édit.), Commentaire de la Loi fédérale sur l'égalité, Genève 2011, p. 97-123.

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

MONDINI ANDREA, Internet et courriel au travail, TREX – L'expert fiduciaire 2005, p. 364-366.

MOREILLON LAURENT, Nouveaux délits informatiques sur Internet, medialex 1/01, p. 21-26.

ORDOLLI GENEVIÈVE, Intranet et internet dans les rapports collectifs de travail – Etude de droit suisse et de droit comparé, Genève 2013.

PASCHE JEAN-MARC, La politique des entreprises, in : PERRIN (édit.), Internet au lieu de travail, Lausanne 2004, p. 67-79.

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).

PORTMANN WOLFGANG, Commentaire des articles 319 à 362 CO, in : HONSELL/VOGT/WIEGAND, Basler Kommentar, Obligationenrecht I, Bâle 2011.

RUDOLPH/VON KAENEL, Aktuelle Fragen zur Arbeitszeit, PJA 2012, p. 197-207.

SANTORO DIMITRI, Die Konventionalstrafe im Arbeitsvertrag, Berne 2001.

SONNENBERG CAROLE, La protection de la personnalité du travailleur : sauvegarde de sa santé et sécurité au travail, Lausanne 2010.

STOLL DANIEL, Quelques considérations de droit pénal, in : PERRIN (édit.), Internet au lieu de travail, Lausanne 2004, p. 109-132.

STREIFF/VON KAENEL/RUDOLPH, Arbeitsvertrag, Praxiskommentar zu Art. 319-362 OR, 7e éd., Zurich 2012.

STUTZ/GEIGER-STEINER, Arbeitsrechtliche Fragen rund um Social Media, Revue de l'avocat 2013, p. 212-216.

SUBILIA OLIVIER, La relation de travail : quelques problèmes pratiques, in : PERRIN (édit.), Internet au lieu de travail, Lausanne 2004, p. 37-65.

SUBILIA/DUC, Droit du travail – Eléments de droit suisse, 2e éd., Lausanne 2010.

VON KAENEL ADRIAN, Internet und Datenschutz am Arbeitsplatz, in : Geschäftsplattform Internet II, Zurich 2001, p. 21-47 (cité : VON KAENEL, Internet).

VON KAENEL ADRIAN, Die ständige Erreichbarkeit des Arbeitnehmers, DTA 2009, p. 1-9 (cité : VON KAENEL, Erreichbarkeit).

WENNUBST GABRIELLA, Mobbing – Le harcèlement psychologique analysé sur le lieu de travail, Lausanne 1999.

WERRO FRANZ, La peine conventionnelle : quelques aspects saillants de l'actualité jurisprudentielle, in : La pratique contractuelle 2 – Symposium en droit des contrats, Genève/Zurich/Bâle 2011, p. 1-19.

WYLER RÉMY, Droit du travail, 2e éd., Berne 2008.

CHRISTIAN FLUECKIGER*

La *googlelisation* des employés respecte-t-elle les principes de la protection des données ?

Sommaire

		Page
I.	Introduction	74
II.	Traitements de données causés par une *googlelisation*	75
III.	Règles applicables à la *googlelisation* des employés	77
	A. En droit privé	77
	1. Article 328*b* CO	77
	a) Application de l'article 328*b* CO dans le temps	78
	b) Articulation entre l'article 328*b* CO et la LPD	78
	2. La Loi fédérale sur la protection des données (LPD)	79
	B. En droit public	79
IV.	Principes généraux applicables à la *googlelisation* des employés	80
	A. Licéité	81
	1. Droit privé	81
	2. Droit public	81
	B. Proportionnalité	81
	C. Finalité	82
	D. Reconnaissabilité des traitements et de la finalité	83
	E. Exactitude	83
	F. Sécurité des données	84
	G. Communications transfrontières	85
	H. Devoir d'informer et droit d'accès	87
V.	Motifs pouvant justifier une atteinte illicite à la personnalité	88
VI.	Articulations entre les principes et les motifs justificatifs	89
VII.	La *googlelisation* cause-t-elle une atteinte illicite injustifiée à la personnalité des employés ?	92
	A. En droit privé	92
	B. En droit public	92

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

VIII. Est-il possible d'effectuer une *googlelisation* conforme à la protection des données ? 93
A. En droit privé 93
B. En droit public 94
IX. Est-il possible de freiner les *googlelisations* ? 95
X. Conclusions 96
XI. Bibliographie 97

I. Introduction

Entre 2010 et 2012, des études réalisées d'après un sondage interrogeant entre 490 et 837 recruteurs dans huit pays européens constatent que 68% à 71% d'entre eux *googlelisent*[1] les candidats[2], alors qu'ils n'étaient que 36% avant 2010. En avril 2013, le CEO d'une entreprise de recrutement déclarait dans un entretien au Figaro que « *Aujourd'hui, le premier réflexe préalable à une rencontre est de taper le nom de la personne sur les moteurs de recherche. Ainsi, les rencontres entre deux parfaits inconnus se raréfient* »[3].

De manière plus générale, les recherches de noms de personnes représentent aujourd'hui une requête sur cinq sur Google, qui détennait en 2011 environ le 90% des parts du marché des moteurs de recherche[4].

Au vu de ces chiffres, il est à craindre une généralisation de cette pratique. Mais est-elle conforme aux règles et principes de la protection des données personnelles ?

Il est d'usage d'entendre que toutes les données personnelles mises à disposition sur Internet par les candidats/employés deviennent publiques et sont susceptibles d'être traitées par tout un chacun et a fortiori par les recruteurs/employeurs. Mais comme cette

1 Par googlelisation, il faut comprendre la recherche d'informations sur une personne avec les moteurs de recherches, les réseaux sociaux ou d'autres services Internet.

2 http://www.blogdumoderateur.com/enquete-limpact-des-reseaux-sociaux-sur-le-recrutement-et-la-recherche-demploi ; http://www.stepstone.be/A-propos-de-StepStone/loader.cfm?csModule=security/getfile&pageid=16901 ; http://www.20min.ch/ro/life/lifestyle/story/29704100 (consultés le 14.01.2014).

3 Déclaration de Jacques Froissant, CEO du cabinet de recrutement 2.0 Altaïde, in : http://www.lefigaro.fr/emploi/2013/04/09/09005-20130409ARTFIG00385-dans-le-recrutement-la-notion-de-mystere-a-disparu.php (consulté le 14.01.2014).

4 RUIZ, p. 87 s.

contribution tentera de le démontrer, c'est une « croyance populaire » à laquelle les règles sur la protection des données s'efforcent de tordre le cou.

Les recruteurs/employeurs ne sont pas en droit de rechercher des informations sur un candidat/employé avec des moteurs de recherche, à travers des réseaux sociaux ou d'autres services Internet.

Cette restriction provoquera sans aucun doute un débat, mais quoi qu'il en soit, il s'agira de déterminer quels sont les moyens que peuvent utiliser les candidats/employés pour faire respecter leurs droits en matière de protection des données, dans la mesure où ces moyens existent.

Les questions traitées ci-après sont moins abstraites qu'il n'y paraît puisque, déjà en 2009, une employée de la compagnie d'assurance Nationale Suisse se faisait licencier, son employeur ayant constaté qu'elle utilisait un réseau social, alors qu'elle était censée rester dans l'obscurité durant son arrêt maladie[5]. Sans compter les entreprises Ikea, Euro Disney, Lidl et Aldi qui sont accusées d'avoir engagé des professionnels pour se renseigner sur des candidats/employés[6]. Certes, dans ces cas-là les employeurs sont allés beaucoup plus loin que la simple utilisation d'Internet, en engageant notamment des détectives, mais qui peut le plus peut le moins. Autrement dit, si des entreprises sont prêtes à utiliser de tels moyens, il n'est pas exagéré de penser que beaucoup d'autres se contentent de simplement *googleliser* leurs candidats/employés.

À relever enfin que les tribunaux voient de plus en plus de preuves provenant de réseaux sociaux.

II. Traitements de données causés par une *googlelisation*

Lorsqu'un recruteur/employeur effectue une recherche sur un candidat/employé en utilisant des services tels que Google, Facebook, etc., il est d'usage de s'arrêter sur les données qu'il récolte. Cependant, il est rare que l'on s'attarde sur l'aspect « communication aux tiers » que provoque cette recherche.

Or, il s'agit là d'un problème non négligeable en matière de protection des données puisqu'il s'agit d'une communication de données personnelles à des tiers à l'étranger et

5 http://news.bbc.co.uk/2/hi/8018329.stm (consulté le 14.01.2014).

6 http://www.letemps.ch/Page/Uuid/7e76edfe-5b3e-11e2-b91b-db7740915aad|0#.UhYYyH-gaZQ (consulté le 14.01.2014).

que de surcroît les services utilisés pour *googleliser* des candidats/employés contribuent, pour la plupart d'entre eux, à profiler[7] les individus recherchant et recherchés.

La simple saisie des nom et prénom d'un candidat/employé par un recruteur/employeur constitue en fait une transmission de nombreuses autres données personnelles. Sauf lorsque des mesures draconiennes sont prises, ce qui est rarement le cas, le service utilisé sait que la personne derrière l'écran est un recruteur/employeur et que la personne *googlelisée* est un candidat/employé. Il connaît aussi leur identité et d'autres détails sur leur vie privée/publique.

Ces déductions sont le fruit de recoupements d'informations laissées au fur et à mesure de l'utilisation d'Internet. Les personnes sceptiques qui pensent être restées anonymes ne sont pas conscientes des innombrables traces cumulées stockées sur le net. Par exemple, Google saura qu'une femme est enceinte avant qu'elle le dise ; Google saura qu'un enfant souffre d'une maladie génétique, même si ses parents cachent l'information, sachant que 2/3 des internautes utilisent ce moteur de recherche pour obtenir des informations sur leurs préoccupations.

Aujourd'hui, le réflexe de chacun étant de se renseigner sur la toile, les personnes laissent automatiquement, la plus part du temps, des traces non anonymisées, même si elles pensent avoir pris des précautions.

L'ajout du module complémentaire gratuit « collusion » au navigateur Firefox permet de constater que, par exemple, la simple consultation du site www.lemonde.fr provoque la communication - à une dizaine d'autres sites - de données personnelles, telles que le fait d'avoir consulté le site en question, les mots clefs utilisés, les pages lues, la durée de lecture, etc.

Plus précisément, la *googlelisation* d'un candidat revient à communiquer, à un ou plusieurs tiers, que cette personne a postulé pour un nouvel emploi, ainsi que d'autres données personnelles ; la *googlelisation* de l'employé indique non seulement qu'on le surveille, mais peut-être également les raisons de cette surveillance.

Or, quelles sont les garanties que ces informations ne viendront pas aux oreilles de personnes à qui le postulant/l'employé voulait cacher sa démarche ?

Certes cela peut paraître à première vue un risque très peu probable. Cependant, qui peut garantir que les sociétés de recrutement ou les employeurs ne cherchent pas à acheter des données de candidats/employés aux sociétés de service du net ?

---

[7] Assemblage de données qui permet d'apprécier les caractéristiques essentielles de la personnalité d'une personne physique, par exemple son mode de comportement et ses habitudes de consommation (art. 3 LPD ; RS 235.1).

Les exemples d'Euro Disney, Ikea, Lidl et Aldi cités en introduction, ainsi que tous ceux qui n'ont pas été découverts ou relayés par la presse, crédibilisent ce genre d'hypothèses et permettent parfois de diminuer le nombre de personnes qui les qualifient « d'émanations de paranoïaques » ou « d'Ayatollah de la protection des données ».

Enfin, rappelons que la Commission française Nationale de l'Informatique et des Libertés (CNIL) a demandé à Google en 2007 de limiter dans le temps le stockage des données des utilisateurs[8]. Or, le 20 juin 2013, les autorités de protection des données d'Allemagne, d'Espagne, de France (CNIL), d'Italie, des Pays-Bas et du Royaume Uni ont mis cette compagnie en demeure de répondre à un certain nombre de questions sur le traitement des données effectué[9]. Google refusant de se soumettre aux autorités, un bras de fer a commencé[10].

III. Règles applicables à la *googlelisation* des employés

A. En droit privé

1. Article 328*b* CO

Les recruteurs/employeurs ne sont en droit, selon l'article 328*b* CO, de « traiter des données concernant les travailleurs 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 »[11].

L'application de cette disposition dans le cadre du sujet traité soulève notamment deux questions, qui ont déjà fait couler un peu d'encre. Cet article est-il applicable avant la conclusion du contrat de travail et quelle est son articulation avec la Loi fédérale sur la protection des données (LPD)[12] ?

8 http://juridique.isonline.fr/2007/03/18/google-rendra-anonymes-les-donnees-recoltees-sur-ses-utilisateurs-3/ (consulté le 14.01.2014).

9 http://www.cnil.fr/linstitution/actualite/article/article/la-cnil-met-en-demeure-google-de-se-conformer-dans-un-delai-de-trois-mois-a-la-loi-informatique (consulté le 14.01.2014).

10 http://www.lemondedudroit.fr/decryptages-profession-avocat/179489-google-va-etre-sanctionne-par-la-cnil-.html (consulté le 14.01.2014).

11 RS 220.

12 RS 235.1.

a) Application de l'article 328*b* CO dans le temps

Vu que l'article 328*b* CO se trouve dans les dispositions concernant le contrat de travail, se pose légitimement la question de savoir s'il s'applique aux données traitées relatives aux postulants à un nouvel emploi ?

La doctrine minoritaire affirme que cette disposition n'est pas applicable aux rapports précontractuels[13]. Le Tribunal fédéral a clos le débat puisqu'il a jugé qu'elle « *interdit à l'employeur, avant d'engager un candidat, de lui poser des questions qui n'ont pas trait au poste de travail ou à l'activité à exercer et qui portent atteinte à sa sphère privée* »[14]. Il confirme ainsi l'avis de la doctrine majoritaire[15] ainsi qu'un arrêt allant déjà dans ce sens, rendu vingt ans auparavant[16].

b) Articulation entre l'article 328*b* CO et la LPD

L'articulation entre l'article 328*b* CO et la LPD fait aussi l'objet d'un débat[17]. Est-ce un simple rappel des principes généraux de la LPD ? Une *lex specialis* de l'article 13 al. 2 let. a LPD ? Une concrétisation des principes de la finalité et de la proportionnalité figurant à l'article 4 al. 2 et 3 LPD ? Ou une dérogation à la LPD[18] ? Le Tribunal fédéral semble à nouveau avoir tranché puisqu'il a jugé que cette disposition constitue la présomption légale que les données des candidats/employés portant sur leurs aptitudes à remplir leur emploi, ou étant nécessaires à l'exécution du contrat, ne portent pas atteinte à leur personnalité[19]. Par cet arrêt, il fait sienne la théorie que l'article 328*b* CO introduit le principe de l'illicéité pour le traitement de données personnelles des candidats/ employés par le recruteur/employeur et celui de la présomption de licéité dans deux cas de figure seulement : « *d'une part, si les informations intéressent les aptitudes du travailleur à remplir son emploi ; d'autre part, si elles sont nécessaires à l'exécution du contrat de travail* »[20]. En d'autres termes, cette disposition appartient à la fois à la loi

13 MEIER, N 2068, et réf. citées, p. 660.
14 Arrêt du TF 2C_103/2008 du 30 juin 2008, consid. 6.2 ; voir aussi DUNAND, N 5 s., p. 319 s.
15 BALZAN, p. 9 s. et réf. citées ; CONSEIL FÉDÉRAL, p. 58.
16 ATF 122 V 267, consid. 3b ; FLUECKIGER, Dopage, N 316 et réf. citées, p. 97 ; MEIER, N 2068 et réf. citées, p. 660 ; SUBILIA/DUC, N 12, p. 342.
17 Voir BALZAN, p. 5 s., et réf. citées ; DUNAND, N 4, p. 319 ; MEIER, N 2032 ss et réf. citées, p. 650 ; SUBILIA/DUC, N 10, p. 341 s.
18 BALZAN, p. 5 s.
19 ATF 130 II 425, consid. 3.3.
20 AUBERT, p. 149 s. ; voir dans le même sens DUNAND, N 4, p. 319.

constituant un des trois motifs justificatifs figurant à l'article 13 al. 1 LPD[21] et à celle des traitements illicites interdits par l'article 4 al. 1 LPD[22].

Ce choix du Tribunal fédéral a l'avantage d'offrir une articulation cohérente entre l'article 328*b* CO et la LPD. Par exemple, si une banque s'adresse à un employeur pour demander le salaire d'un employé voulant contracter un emprunt hypothécaire[23], il permet de déclarer cette communication illicite. Alors que la seule application de la LPD l'autoriserait ; de même si l'on considère que l'article 328*b* CO n'est qu'un motif justificatif. Dans ce cas, il suffit de laisser cette disposition de côté et d'invoquer l'intérêt privé prépondérant de la banque qui permettra également de juger le traitement de données proportionné.

L'interprétation choisie par nos juges fédéraux est l'une des rares qui permette de considérer clairement comme illicite cette communication. Celle consistant à considérer que l'article 328*b* CO est une concrétisation de l'article 4 al. 2 et 3 LPD l'interdirait désormais également au vu de l'arrêt Logistep du Tribunal fédéral[24], qui impose l'application des motifs justificatifs avec retenue. Ainsi, il ne serait pas possible de justifier un traitement de données qui viole l'article 328*b* CO (voir ch. VI).

2. La Loi fédérale sur la protection des données (LPD)

L'examen d'une récolte ou une communication de données par un recruteur/employeur sur Internet doit non seulement se faire à la lumière de l'article 328*b* CO, mais également à celle des principes généraux, des motifs justificatifs et du droit d'accès figurant dans la LPD.

Si l'examen se limitait à la disposition précitée, seules l'étendue et la proportionnalité du traitement de données seraient vérifiées. Or, le recruteur/employeur se doit également et impérativement de respecter notamment l'exactitude des données, le droit d'accès et la sécurisation des données (voir ch. IV).

B. En droit public

Bien que la LPD soit classifiée sous droit privé dans le recueil systématique du droit fédéral, elle contient également des règles de protection des données pour les organes fédéraux. Pour les administrations et autorités cantonales et communales, établissements

21 FLUECKIGER, Dopage, N 307, p. 92 s.
22 ROSENTHAL/JÖHRI, N 4 ss, p. 724.
23 AUBERT, p. 151.
24 ATF 136 II 508, consid. 5.2.4, JdT 2011 II 446.

et collectivités de droit public cantonaux et communaux, ainsi que pour les personnes morales accomplissant des tâches d'intérêt public (ci-après entités publiques), chaque canton possède ses propres règles, relativement similaires de l'un à l'autre[25].

En droit privé, un traitement de données ne doit pas être contraire à une loi et respecter les principes de la protection des données. Alors qu'en droit public, un traitement de données ne peut exister que si une base légale le prévoit, qu'il est nécessaire à l'accomplissement d'une tâche légale ou que la personne concernée y a consenti, par exemple en rendant ses données accessibles à tout un chacun, et qu'il respecte aussi lesdits principes.

En raison de cette différence, la plupart des lois cantonales relatives à la protection des données, de même que la LPD, connaissent des dispositions sur les communications, ainsi que les traitements à des fins de recherche, de planification et de statistique.

Cette distinction provoque aussi deux démarches différentes : en droit privé il faut, dans un premier temps, vérifier qu'aucune loi n'interdise le traitement, alors qu'en droit public il faut préalablement trouver la base légale autorisant expressément le traitement ou indiquant la tâche légale qui le rend nécessaire.

S'ajoute à ces dispositions cantonales sur la protection des données, le devoir de respecter le secret de fonction.

Hormis ces principales particularités, l'application des règles et principes de la protection des données ne diffère pas beaucoup entre le droit privé et le droit public.

IV. Principes généraux applicables à la *googlelisation* des employés

La loi fédérale et les lois cantonales imposent le respect de plusieurs principes afin que les traitements de données personnelles respectent la personnalité des personnes concernées.

Excepté pour celui de la licéité qui est différent en droit public (voir ch. III.B), les précisions d'application pour les principes généraux de la protection des données, figurant notamment aux articles 4 à 10 LPD pour les personnes privées ainsi que les

[25] Pour plus de détails voir : http://www.edoeb.admin.ch/dokumentation/00614/index.html?lang=fr. (consulté le 14.01.2014).

organes de la Confédération, sont aussi valables pour les traitements de données soumis au droit cantonal, puisqu'ils ont été repris par tous les cantons.

L'examen détaillé, principe par principe, exposé ci-après permet de conclure que tous les traitements de données dus à la *googlelisation* des candidats/employés ont la particularité d'enfreindre presque tous les principes. À noter qu'il est rarissime qu'un traitement de données aussi bien implanté et couramment effectué arrive à un score aussi navrant.

A. Licéité

1. Droit privé

Comme affirmé sous le ch. III.A.1.b), l'article 328*b* CO déclare illicite tous les traitements qui ne sont pas directement liés aux aptitudes du candidat/employé à remplir son emploi ou qui sont nécessaires à l'exécution du contrat de travail.

Par conséquent, une *googlelisation* du candidat/employé respecte ce principe pour autant que les données récoltées ou lues restent dans le champ des traitements licites[26].

Or, il est difficilement concevable que lors d'une telle recherche, il soit possible de trier ou de faire abstraction des données strictement privées[27].

2. Droit public

Compte tenu de l'exigence du respect du principe de la légalité imposée par le droit public, toutes les personnes soumises au secret de fonction et s'occupant des ressources humaines devraient bénéficier d'une base légale pour *googleliser* les candidats/employés ou à tout le moins justifier que cela soit nécessaire pour l'accomplissement d'une tâche légale. Faute de quoi, une *googlelisation* constitue une communication à des tiers sans légitimation et par conséquent est un traitement de données illicite et pourrait même être dénoncé dans certains cas pour violation du secret de fonction, à tout le moins par dol éventuel.

B. Proportionnalité

L'examen de la proportionnalité est cadré par la délimitation des traitements de données jugés licites effectués par les recruteurs/employeurs et inscrite à l'article 328*b* CO.

26 CONSEIL FÉDÉRAL, p. 58.
27 CONSEIL FÉDÉRAL, p. 58.

Autrement dit, seuls deux buts doivent être pris en compte – jugement de l'aptitude du travailleur et de la bonne exécution du contrat de travail – pour vérifier si les trois composantes du principe en cause sont respectées[28].

– La *googlelisation* est-elle apte à atteindre les deux buts précités ? Rien n'est moins sûr. Le recruteur/employeur risque de se forger une opinion sur des données incomplètes, voire inexactes. Sorties du contexte, les informations peuvent être très mal interprétées. Mais surtout, le recruteur/employeur consultera, nécessairement, davantage de données que ne le lui permet l'article 328*b* CO.
– Existe-t-il d'autres moyens moins dommageables pour la personnalité des candidats/employés permettant d'atteindre les mêmes buts ? De toute évidence, la réponse est positive. L'évaluation des candidats/employés n'a certainement pas attendu la *googlelisation* pour être efficace. Certes, des recruteurs diront qu'en *googlelisant* le candidat ils ont découvert une caractéristique de l'employé incompatible avec l'exercice de l'activité. Cette affirmation justifie-t-elle l'utilisation d'un tel moyen ? Ou est-ce plutôt l'aveu inconscient que cet outil a permis de palier aux défauts d'examens/questionnaires d'entretien d'embauche de mauvaise qualité ?

Vu la réponse clairement positive à cette dernière question, il n'est pas utile d'examiner la prépondérance de l'intérêt du recruteur/employeur par rapport à celui de l'employé. Même si la réponse était négative cela conduirait au constat qu'aucune composante du principe de la proportionnalité n'est respectée en l'espèce.

C. Finalité

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[29].

Dans le cadre de la *googlelisation* d'un candidat/employé, les buts autorisés figurent exhaustivement dans l'article 328*b* CO et se limitent au jugement de l'aptitude du travailleur et à la bonne exécution du contrat de travail. Il n'est dès lors pas nécessaire de les annoncer.

Il n'empêche qu'une *googlelisation* viole le principe de la finalité puisqu'elle récolte forcément des données n'entrant pas dans le cadre restreint de l'article 328*b* CO, même si la personne concernée est préalablement informée[30].

---

28 FLUECKIGER, Contrôles antidopage, p. 686.
29 Art. 4 al. 3 LPD ; MAURER-LAMBROU/STEINER, p. 82 ss ; ROSENTHAL/JÖHRI, N 31 ss, p. 89 ss.

D. Reconnaissabilité des traitements et de la finalité

Les traitements de données et leur finalité doivent être reconnaissables par les candidats/employés[31], même lorsque les données ne sont pas récoltées directement auprès des personnes concernées. Pour ce faire, le recruteur/employeur doit informer ces dernières au plus tard lors de l'enregistrement des données ou, en l'absence d'enregistrement, lors de la première communication à un tiers[32].

Or en pratique, il est d'usage de *googleliser* ces personnes sans jamais les en informer. Cependant, compte tenu qu'une *googlelisation* constitue une communication de données à des tiers, l'absence ou non d'enregistrement n'entre pas en ligne de compte et les candidats/employés doivent être informés avant que la recherche soit effectuée pour que ce principe soit respecté. Par exemple, il faudrait que les recruteurs/employeurs mentionnent clairement aux personnes concernées qu'ils effectueront ces recherches, sans qu'il soit obligatoire d'indiquer les raisons (voir ch. IV.C) dans la mise au concours, lors de l'entretien d'embauche ou dans le règlement d'entreprise en ce qui concerne les employés.

E. Exactitude

Un recruteur/employeur qui traite des données personnelles doit s'assurer qu'elles sont correctes. Il doit prendre toute mesure appropriée permettant d'effacer ou de rectifier les données inexactes ou incomplètes au regard des finalités pour lesquelles elles sont collectées ou traitées[33]. En cas de contestation, il devra prouver qu'il s'est assuré de l'exactitude des données[34]. Bien évidemment, les candidats/employés concernés peuvent requérir la rectification des données inexactes[35].

La *googlelisation* des candidats/employés, telle qu'usuellement pratiquée aujourd'hui, ne respecte clairement pas ce principe. S'il venait à l'esprit des recruteurs de le respecter, ils devraient à tout le moins laisser la personne s'expliquer sur toutes les informations récoltées, puisque la plupart recueillies sur Internet ne sont pas fiables, après évidemment avoir écarté celles qui n'entrent pas dans le cadre délimité par l'article 328*b* CO. Par écarter il faut comprendre non seulement effacer, mais également « oublier »,

---

30 MEIER, N 732, p. 286.
31 Art. 4 al. 4 LPD ; ROSENTHAL/JÖHRI, N 51 ss, p. 96 ss.
32 MEIER, N 706, p. 277 ; CONSEIL FÉDÉRAL, p. 58.
33 Art. 5 LPD ; MAURER-LAMBROU, N 1 ss, p. 92 ss ; ROSENTHAL/JÖHRI, N 1 ss, p. 124 ss.
34 MEIER, N 760, p. 293.
35 Art. 5 al. 2 LPD ; MAURER-LAMBROU, N 14 ss, p. 96 ss ; ROSENTHAL/JÖHRI, N 12 ss, p. 128 ss.

c'est-à-dire que les données ne doivent être prises en compte en aucune manière dans la relation de travail.

Il est d'autant moins possible de respecter ce principe, pour les petites entreprises, que souvent les casquettes de responsable des ressources humaines et de chef direct sont portées par la même personne. Il lui sera ainsi difficile de faire abstraction des données ne devant pas être récoltées dans ses relations de travail quotidiennes.

De telles contraintes rendent une fois de plus la *googlelisation* nettement moins attractive.

F. Sécurité des données

Le respect de la sécurité des données implique que le recruteur/employeur qui traite des données personnelles ou qui met à disposition un réseau télématique assure la confidentialité, la disponibilité et l'intégrité des données afin de garantir de manière appropriée la protection des données. Il protège les systèmes notamment contre les risques de destruction accidentelle ou non autorisée, perte accidentelle, erreurs techniques, falsification, vol ou utilisation illicite, modification, copie, accès ou autre traitement non autorisés. Pour être appropriées, les mesures techniques et organisationnelles tiennent compte en particulier des critères, tels que le but du traitement de données, la nature et l'étendue du traitement de données, l'évaluation des risques potentiels pour les personnes concernées et le développement technique[36].

Or, la seule lecture de la presse permet d'affirmer que les données livrées sur Internet, notamment par la *googlelisation*, ne bénéficient d'aucune sécurité semblable à celle exigée, sauf lorsqu'il est pris des précautions très particulières que la majorité des utilisateurs ne prennent pas, ni ne connaissent.

Trois exemples suffiront certainement à convaincre les sceptiques. Tout d'abord, le gouvernement américain, par l'intermédiaire de son agence nationale de sécurité (NSA), a notamment mis sur pied les programmes PRISM[37], XKeyscore[38], BullBurn[39] et

36 Art. 8 OLPD.

37 http://www.lemonde.fr/societe/article/2013/07/04/revelations-sur-le-big-brother-francais_3441973_3224.html (consulté le 14.01.2014).

38 http://www.lemonde.fr/international/article/2013/08/02/l-outil-qui-permet-de-detecter-quasiment-tout-ce-que-fait-un-individu-sur-internet_3456856_3210.html (consulté le 14.01.2014).

39 http://www.rts.ch/info/monde/5189004-la-nsa-americaine-dechiffre-les-echanges-cryptes-sur-internet.html (consulté le 14.01.2014).

Muscular[40], permettant de surveiller l'utilisation d'Internet de tous les internautes, y compris les communications cryptées. Ensuite, l'entreprise Google a déclaré devant un tribunal américain que « *vous ne pouvez pas vous attendre à une conversation privée en envoyant un message à Gmail* »[41]. Si la vie privée n'est pas respectée lors de l'utilisation d'une messagerie donnant tous les aspects d'un compte sécurisé et totalement privé, pensez-vous qu'elle le sera pour les données laissées lors des *googlelisations* ?

Enfin, la déclaration du porte-parole de Facebook reconnaissant que : « Nous avons revu nos explications sur la manière dont votre nom, votre photo de profil et son contenu pouvaient être utilisés en relation avec des publicités afin de clarifier le fait que vous autorisez Facebook à les exploiter quand vous utilisez nos services ».

Rappelons pour l'anecdote que ces aspects-là avaient même échappé au général David Petraeus, directeur démissionnaire de la CIA en novembre 2012 en raison d'une liaison extraconjugale, puisqu'il utilisait la messagerie Gmail pour communiquer avec sa maîtresse[42].

G. Communications transfrontières

En saisissant des mots clefs relatifs à des candidats/employés (par exemple, Jean Némar, ivre, nu, blog, …) pour effectuer une *googlelisation* sur divers services, dont les serveurs sont implantés à l'étranger, le recruteur/employeur effectue-t-il une communication transfrontière ?

L'article 5 de l'Ordonnance relative à la Loi fédérale sur la protection des données (OLPD)[43] prévoit que la publication de données personnelles au moyen de services d'information et de communication automatisés afin d'informer le public n'est pas assimilée à une communication à l'étranger. Cependant, « *la communication de données qui ne sont généralement pas accessibles sur un site internet (par ex. cookies, adresse IP) par le biais d'internet remplissent en revanche les critères de flux transfrontière* […] »[44]. La communication de données sur les candidats/employés par l'intermédiaire d'une *googlelisation* doit donc être qualifiée de transfrontière.

---

40 http://www.rts.ch/info/monde/5336617-la-nsa-intercepterait-des-donnees-d-utilisateurs-de-google-et-yahoo.html (consulté le 14.01.2014).

41 http://www.lemonde.fr/technologies/article/2013/08/15/polemique-autour-du-respect-de-la-vie-privee-par-gmail_3462111_651865.html (consulté le 14.01.2014).

42 http://www.lefigaro.fr/international/2012/11/11/01003-20121111ARTFIG00141-la-liaison-dangereuse-du-general-americain-petraeus.php (consulté le 14.01.2014).

43 RS 235.11.

44 MEIER, N 1277, p. 444.

Or, 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. Néanmoins, le cas échéant, des données personnelles peuvent être communiquées à l'étranger, si une des conditions prévues dans les législations de protection des données est remplie[45]. Seules trois, pouvant entrer en ligne de compte en l'espèce, méritent un examen détaillé :

– Tout d'abord, la personne doit avoir donné son consentement[46]. Ce dernier n'est valable que si le candidat/employé exprime sa volonté librement et après avoir été dûment informé. Lorsqu'il s'agit de données sensibles et de profils de la personnalité, son consentement doit être au surplus explicite[47]. On peut présumer que ce n'est jamais le cas, la *googlelisation* se faisant généralement dans le dos du candidat/employé.
– Ensuite, le traitement doit être en relation directe avec la conclusion ou l'exécution d'un contrat et les données traitées doivent concerner le cocontractant[48]. Toutefois, le message du Conseil fédéral précise que la communication en question doit être indispensable[49]. Cette précision restreint encore davantage le cadre fixé par l'article 328*b* CO[50] et rend impossible le respect de cette condition dans le domaine particulier examiné dans cette contribution.
– Enfin, la personne concernée a rendu les données accessibles à tout un chacun et elle ne s'est pas opposée formellement au traitement[51]. À ce propos, la doctrine est d'avis que la récolte sur Internet de données d'internautes qui dévoilent leur vie, ne correspond pas au but de ces derniers ; ils ne le font en principe pas pour que les recruteurs/employeurs se renseignent, sauf évidemment lorsqu'il s'agit de sites de recherches d'emploi ou analogues. Il est donc contraire au principe de la bonne foi d'utiliser des données librement accessibles sur Internet dans un autre but que celui pour lequel elles ont été publiées[52].

45 Art. 6 al. 1 et 2 LPD ; MAURER-LAMBROU/STEINER, N 1 ss, p. 99 ss ; ROSENTHAL/JÖHRI, N 1 ss, p. 131 ss.
46 Art. 6 al. 2 let. b LPD ; MAURER-LAMBROU/STEINER, N 30, p. 109 ; ROSENTHAL/JÖHRI, N 53 ss, p. 155 ss.
47 Art. 4 al. 5 LPD ; ROSENTHAL/JÖHRI, N 66 ss, p. 103 ss.
48 Art. 6 al. 2 let. c LPD ; ROSENTHAL/JÖHRI, N 57 ss, p. 157 s.
49 FF 2003 1915, p. 1941.
50 MEIER, N 1359, p. 465.
51 Art. 6 al. 2 let. f LPD ; ROSENTHAL/JÖHRI, N 75, p. 164.
52 MEIER, N 1589 ss et les réf. citées, p. 527.

Relevons finalement que le *Safe Harbor Privacy Network* conclu avec les USA est remis en cause par la vice-présidente de la Commission européenne, Viviane Reding[53]. Autrement dit, les USA ne seront peut-être plus jugés comme un État offrant une protection des données similaire à la nôtre et qu'une communication vers ce pays devra impérativement passer par le respect d'une des conditions précitées.

H. Devoir d'informer et droit d'accès

Il n'est pas rare qu'une *googlelisation* puisse constituer un profil de la personnalité, c'est-à-dire un assemblage de données permettant d'apprécier les caractéristiques essentielles de la personnalité des candidats/employés, si ceux-ci ne sont pas assez discrets, telles que la réunion d'informations détaillées relatives à l'origine, au revenu, à la fortune, à la formation, aux activités professionnelles, aux connaissances linguistiques, aux relations familiales, aux loisirs, à la réputation, etc.[54]. Elle peut aussi permettre de récolter des données sensibles, telles que celles relatives à la santé, la sphère intime, à l'appartenance à une race, des mesures d'aide sociale, des poursuites ou sanctions pénales et administratives, ainsi qu'aux opinions ou activités religieuses, philosophiques, politiques ou syndicales[55].

Le cas échéant, le recruteur/employeur a l'obligation d'informer le candidat/employé d'une telle collecte le concernant au plus tard lors de la *googlelisation* puisque ce genre de service enregistre instantanément toutes les requêtes. L'information doit au moins contenir l'identité du maître du fichier, les finalités du traitement pour lequel les données sont collectées et les catégories de destinataires des données si la communication des données est envisagée[56].

Même lorsqu'il ne s'agit pas de données sensibles ou de profils de la personnalité, sitôt que le recruteur/employeur enregistre les informations récoltées sur les candidats/ employés par une *googlelisation*, il se doit de respecter leur droit d'accès. A la demande de ces derniers, il doit leur communiquer toutes les données les concernant contenues dans le fichier, y compris les informations disponibles sur l'origine des données, le but et éventuellement la base juridique du traitement, ainsi que les catégories de données

53 http://www.liberation.fr/monde/2013/08/19/affaire-prism-les-cnil-europeennes-saisissent-bruxelles_925609 (consulté le 14.01.2014).

54 RJJ 2006, p. 34, consid. 3.3 ; ATF 129 I 232, consid. 4.3.2, JdT 2004 I 588, SJ 2003 I 513 ; MEIER, N 514, n. 585, p. 227.

55 Art. 3 let. c LPD ; BELSER, N 10 ss, p. 66 s. ; ROSENTHAL/JÖHRI, N 42 ss, p. 40 ss.

56 Art. 14 LPD.

personnelles traitées, de participants au fichier et de destinataires des données[57]. En l'occurrence aucune exception ne peut être invoquée pour refuser le droit d'accès, y compris celle d'une récolte pour un usage exclusivement personnel[58]. Les renseignements sont, en règle générale, fournis gratuitement et par écrit, sous forme d'imprimé ou de photocopie[59].

V. Motifs pouvant justifier une atteinte illicite à la personnalité

Un traitement de données qui porte une atteinte à la personnalité est présumé illicite, sauf s'il bénéficie d'un motif justificatif[60]. Une telle atteinte est réalisée lorsque le traitement de données personnelles viole les principes définis aux art. 4, 5, al. 1, et 7, al. 1 LPD, lorsqu'il s'effectue contre la volonté expresse de la personne concernée ou lorsqu'il s'agit d'une communication à des tiers de données sensibles ou de profils de la personnalité, sans motifs justificatifs[61]. Ces derniers sont les mêmes que pour les atteintes à la personnalité qui ne sont pas causées par un traitement de données, c'est-à-dire la loi, le consentement et l'intérêt public et privé prépondérant[62].

En ce qui concerne la loi, l'article 328*b* CO en constitue une, légitimant les traitements de données dans le cadre des relations de travail qui se limitent à ceux relatifs aux aptitudes du travailleur à remplir son emploi et à l'exécution du contrat de travail (voir ch. III.A.I.b).

Quant au consentement des candidats/employés, même s'il était demandé avant de les *googleliser*, se poserait la question de sa validité, puisqu'il doit être donné librement. Or, dans le cadre des rapports de travail, c'est rarement le cas. En l'occurrence, quel candidat voulant garder ses chances d'obtenir le poste refusera la *googlelisation* ? De surcroît, la doctrine précise « *qu'un travailleur ne peut consentir, même de manière libre, informée, voire explicite* […], *à un traitement de données allant au-delà de l'article 328b CO, que*

57 Art. 8 LPD ; GRAMIGNA/MAURER-LAMBROU, N 21 ss, p. 132 ss ; ROSENTHAL/JÖHRI, N 1 ss, p. 199 ss.

58 Art. 2 al. 2 let. a et 9 LPD ; MAURER-LAMBROU/KUNZ, N 20 ss, p. 50 ; GRAMIGNA/MAURER-LAMBROU, N 1 ss, p. 149 ss ; ROSENTHAL/JÖHRI, N 21 ss, p. 11 s., et N 1 ss, p. 210 ss.

59 Art. 8 al. 5 LPD ; GRAMIGNA/MAURER-LAMBROU, N 56 ss, p. 142 ss ; ROSENTHAL/JÖHRI, N 26, p. 208 s.

60 Art. 13 al. 1 LPD ; RAMPINI, N 1 ss , p. 191 ss ; ROSENTHAL/JÖHRI, N 1 ss, p. 385 ss.

61 Art. 12 LPD ; RAMPINI, N 1 ss, p. 183 ss ; ROSENTHAL/JÖHRI, N 1 ss, p. 350 ss.

62 Art. 13 LPD ; RAMPINI, N 1 ss, p. 191 ss ; ROSENTHAL/JÖHRI, N 1 ss, p. 385 ss.

dans les limites des articles 341 et 362 CO »[63]. Autrement dit, il faudrait que la *googlelisation* ne soit pas effectuée au détriment des candidats/employés pour que le consentement puisse être valable. 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. Cette affirmation est d'autant plus évidente pour les employés qu'il s'agit purement et simplement d'une surveillance débordant du cadre restreint de l'article 328*b* CO.

Au surplus, comme il a été exposé sous le principe des communications transfrontières (voir ch. IV.G), il est contraire au principe de la bonne foi d'utiliser des données, rendues librement accessibles sur Internet, dans un autre but que celui pour lequel elles ont été publiées. L'exception prévue à l'article 12 al. 3 LPD – traitements autorisés des données mises librement à disposition - ne peut donc pas être retenue pour justifier les *googlelisations* des recruteurs/employeurs[64].

Finalement, il est difficile d'imaginer des intérêts publics/privés prépondérants permettant de justifier une *googlelisation* de candidats/employés allant au-delà du cadre restreint fixé par l'article 328*b* CO.

Par conséquent, la *googlelisation* des candidats/employés ne pourrait bénéficier que d'un seul motif justificatif, l'article 328*b* CO, mais dans l'unique cas où elle se pratiquerait dans le cadre très restreint imposé par ce dernier. Autant dire qu'une justification est peu probable, voire impossible, au vu de cette contrainte et de l'état actuel de la technique et des divers moteurs de recherche ou réseaux sociaux.

VI. Articulations entre les principes et les motifs justificatifs

Les articles 28 ss du Code civil (CC) prévoient, comme les règles sur la protection des données (voir ch. V), que « toute atteinte à la personnalité est par définition illicite et habilite la victime à agir pour s'en protéger […] à moins que ne soit réalisé l'un ou l'autre des motifs justificatifs […] »[65]. Le contenu de ces dispositions impose donc de vérifier préalablement si une atteinte à la personnalité est réalisée et le cas échéant, si un

63 DUNAND, N 32, p. 327 ; dans le même sens, MEIER, N 2026, p. 647, et N 2107 ss, p. 677 ss.
64 CONSEIL FÉDÉRAL, p. 58.
65 JEANDIN, N 71, p. 261.

motif justificatif est applicable. Même si en matière de protection des données la présomption est identique, il est plus efficient d'inverser cet ordre de vérification.

Tout d'abord, le Tribunal fédéral a précisé, à propos de l'article 12 LPD définissant les atteintes à la personnalité par des traitements de données, que « *cette disposition doit donc être interprétée en ce sens que la justification d'un traitement de données contrevenant aux principes des art. 4, 5 al. 1 et 7 al. 1 LPD n'est certes pas exclue de manière générale, mais ne peut être admise dans un cas d'espèce qu'avec grande retenue* »[66]. Cette restriction dans l'application des motifs justificatifs, inconnue sous l'angle des articles 28 ss CC, ne permet donc pas de se limiter à un examen binaire - atteinte à la personnalité justifiée ou non - mais en impose un supplémentaire. Selon le degré de violation du principe et les données personnelles en cause, il faut encore s'assurer que le traitement soit justifiable, puisque les justifications ne peuvent s'appliquer « *qu'avec grande retenue* »[67].

Ensuite, les principes de la LPD à ne pas violer contiennent des notions qui recoupent celles contenues dans les motifs justificatifs. Ces étroits recoupements ne se retrouvent pas dans le cadre de l'examen des atteintes à la personnalité soumises exclusivement aux articles 28 ss CC. Plus concrètement, un traitement de données personnelles bénéficiant du motif justificatif d'un intérêt prépondérant public ou privé ne peut pas violer le principe général de la proportionnalité, puisque la prépondérance d'un tel intérêt s'apprécie avec les mêmes critères que ceux intervenant dans l'appréciation dudit principe[68]. Mais avant tout, une collecte de données, sensibles ou non, et la finalité d'un traitement doivent impérativement respecter le principe de la reconnaissabilité par les personnes concernées[69]. Or, la détermination de la violation ou non de ce principe, contrairement à ceux de l'exactitude ou de la sécurité par exemple, conduit forcément à l'examen de l'une des conditions fondamentales pour obtenir un consentement valable, c'est-à-dire l'information préalable de la personne concernée[70].

Pour prouver que les informations nécessaires ont été valablement communiquées, il est recommandé de le faire confirmer par écrit par les personnes concernées. Puisque cette reconnaissance est aussi un des éléments indispensables à l'obtention d'un consentement valable, il est dès lors d'usage d'en profiter pour obtenir un consentement exprès, même s'il n'est pas indispensable[71].

66 ATF 136 II 508, consid. 5.2.4, JdT 2011 II 446.
67 ATF 136 II 508, consid. 5.2.4, JdT 2011 II 446.
68 FLUECKIGER, Dopage, N 311, p. 93.
69 Art. 4 al. 4 LPD ; ROSENTHAL/JÖHRI, N 51 ss, p. 96 ss.
70 Art. 4 al. 5 LPD ; ROSENTHAL/JÖHRI, N 66 ss, p. 103 ss.
71 MEIER, N 714, p. 281.

À ce propos, relevons « que la collecte soit reconnaissable […] ne permet pas d'admettre sans autre un consentement tacite de la personne concernée à une atteinte qui serait portée à sa personnalité par la collecte en question »[72]. Pour qu'un consentement tacite soit admis, il faut que la personne concernée s'attende « selon les informations en sa possession ou selon le cours ordinaire des choses, à ce que de telles données soient collectées et enregistrées par leur destinataire, pour autant qu'elle puisse raisonnablement appréhender les contours du traitement, de sorte que son consentement soit également éclairé »[73].

Par exemple, « par son inscription, la personne concernée consent tacitement au traitement des données personnelles relatives à sa participation à une manifestation sportive (attribution à une catégorie, dossard, envoi des informations pratiques, etc.) ; il en va à notre sens de même, malgré sa portée théoriquement mondiale, pour la publication sur internet de la liste des départs et des classements, mais en revanche pas pour la communication des données (notamment adresses et photographies) à des tiers (par ex. un sponsor) en vue d'utilisation commerciale ou non commerciale. Une telle réutilisation doit être clairement indiquée dans les conditions de participation et les participants doivent avoir la faculté de s'y opposer. À défaut, on ne saurait retenir un consentement tacite de leur part. »[74].

En raison de ces différences et par souci d'efficience, il est dès lors d'usage d'examiner en premier lieu si les atteintes à la personnalité causées par des traitements de données bénéficient d'un motif justificatif, avant de vérifier s'ils violent un principe général, pour déterminer s'ils causent une atteinte illicite[75].

Ainsi, si un traitement ne bénéficie pas d'un des trois motifs justificatifs, il est déclaré illicite et l'examen s'arrête là. Dans le cas contraire, il faut encore vérifier si les principes généraux de la LPD ne sont pas trop gravement violés pour confirmer que le motif retenu s'applique et que le traitement soit jugé licite.

En revanche, si on établit dans un premier temps qu'un traitement respecte les principes généraux de la protection des données, l'examen sera forcément plus long et fastidieux. Non seulement ceux-ci sont plus nombreux que les motifs (pour s'en convaincre il suffit de comparer les parties IV et V), mais ils incluent aussi certaines composantes identiques pouvant déjà être vérifiées lors de l'examen de ces derniers.

---

72 MEIER, N 714, p. 281.
73 MEIER, N 879, p. 334.
74 MEIER, N 879, p. 334 s.
75 DUNAND, N 13, p. 322.

VII. La *googlelisation* cause-t-elle une atteinte illicite injustifiée à la personnalité des employés ?

Conformément aux développements qui précèdent (voir ch. V et VI), il faut commencer par vérifier si la *googlelisation* bénéficie d'un motif justificatif pour les recruteurs/employeurs soumis aux règles de droit privé de la LPD. Pour ceux soumis aux règles de droit public de la LPD ou aux règles cantonales sur la protection des données, il s'agit de vérifier si ce traitement de données personnelles bénéficie d'une base légale ou s'il est nécessaire pour l'accomplissement d'une tâche légale.

A. En droit privé

L'examen des trois motifs justificatifs conduit à la constatation qu'une *googlelisation* n'en bénéficie d'aucun, au vu de la manière dont elle est effectuée usuellement (voir ch. V).

Même si un motif justificatif devait, contre toute attente, être un jour reconnu pour la *googlelisation*, tel qu'un intérêt privé/public prépondérant ou une interprétation très large de l'article 328*b* CO, les atteintes à la personnalité continueraient d'être jugées illicites puisque la jurisprudence du Tribunal fédéral[76] impose d'appliquer avec retenue les motifs justificatifs lorsque des principes généraux sont gravement violés (voir ch. V). Or, le nombre de principes violés et le degré de gravité de l'atteinte à la personnalité des candidats/employés, notamment par la récolte de données sensibles, devraient imposer une retenue conséquente[77].

B. En droit public

Il n'existe évidemment aucune base légale permettant aux entités publiques de recueillir toutes les informations relatives à des candidats/employés accessibles sur Internet. Se pose alors la question de savoir si une *googlelisation* est nécessaire pour accomplir la tâche légale de recruter ou surveiller, respectivement des candidats ou des employés.

Il n'est pas besoin de relire consciencieusement toutes les règles de droit public cantonales et fédérales pour savoir si de telles tâches y figurent. La « lenteur d'adaptation » des dispositions légales est telle qu'il est certain qu'on n'en trouvera

76 ATF 136 II 508, consid. 5.2.4, JdT 2011 II 446.
77 Voir dans ce sens, CONSEIL FÉDÉRAL, p. 58.

aucune contenant une formulation telle que « […] *devra s'assurer en consultant internet que le candidat/employé est …* ». La description de la tâche devra impérativement prévoir l'utilisation de l'outil Internet, vu que des données sensibles sont susceptibles d'être récoltées. Un principe général veut que plus les données traitées sont sensibles, plus la base légale doit être précise. L'exemple précité paraît être un minimum pour le respecter.

Au vu de ce constat, il s'avère que toutes les personnes soumises aux règles cantonales de la protection des données ou aux articles 16 ss de la LPD, qui *googlelisent* les candidats/employés causent une atteinte illicite à la personnalité de ces derniers.

VIII. Est-il possible d'effectuer une *googlelisation* conforme à la protection des données ?

La *googlelisation* portant manifestement atteinte à la personnalité des candidats/employés, se pose alors la question de savoir s'il serait possible, moyennant l'aménagement de quelques modalités, de rendre ce traitement de données personnelles conforme aux règles sur la protection des données.

A. En droit privé

Il semble difficile d'imaginer que les particuliers, les entreprises et tous ceux qui sont soumis aux articles 12 ss LPD pourront un jour *googleliser* des candidats/employés en bénéficiant d'un motif justificatif et en ne violant qu'avec retenue les principes généraux[78].

Il est peu probable que les articles 328*b* et 362 CO soient modifiés pour que ce genre de traitement de données personnelles bénéficie d'une loi ou que le consentement des candidats/employés soit valable, même s'ils acceptent une démarche allant à l'encontre de leurs intérêts.

Tout comme il est difficilement concevable qu'un intérêt public/privé prépondérant surgisse et soit un jour admis.

78 Voir dans ce sens, CONSEIL FÉDÉRAL, p. 58.

Même si ces événements peu plausibles arrivaient, il resterait toujours difficile de ne violer les principes généraux qu'avec la retenue imposée par le Tribunal fédéral[79].

Certes, l'utilisation d'une stratégie de recherche particulière (limitation des mots clefs par exemple) et d'outils informatiques, tels qu'un proxy, permettrait d'envisager de respecter les principes de la sécurité et de la communication transfrontière. Les recruteurs/employeurs éviteraient ainsi de communiquer des informations à Google, Microsoft, Facebook, etc., comme la recherche d'un emploi d'un candidat ou le soupçon qu'un employé a un taux d'absentéisme trop élevé.

Certes, une information préalable des candidats/employés, permettrait de respecter le principe de la reconnaissabilité des traitements et de la finalité.

Il n'empêche qu'il resterait difficile, voire impossible, de respecter suffisamment les principes de la licéité, proportionnalité et exactitude pour répondre aux exigences de la jurisprudence fédérale précitée.

B. En droit public

Les personnes soumises aux règles cantonales de protection des données ou aux articles 16 ss LPD ne peuvent pas, tant et aussi longtemps qu'une base légale formelle ne le prévoit pas directement ou par l'intermédiaire d'une description de tâche légale, *googleliser* les candidats/employés en conformité avec les règles sur la protection des données.

Même si des collectivités avaient des velléités de légiférer dans ce sens, le projet ne passerait probablement pas le contrôle du respect des principes généraux, notamment la proportionnalité, la sécurité et l'exactitude. Imaginer des modalités permettant de *googleliser* dans le respect de ces règles est particulièrement périlleux. Jugerons-nous un jour que les données de la sphère privée soient nécessaires pour l'évaluation d'un candidat/employé ? Existera-t-il un jour l'assurance de l'exactitude des données trouvées sur le net ? Les données cesseront-elles d'être convoitées par la NSA et les « géants américains d'Internet », ou leurs équivalents dans d'autres endroits du globe ?

79 ATF 136 II 508, consid. 5.2.4, JdT 2011 II 446.

IX. Est-il possible de freiner les *googlelisations* ?

Dans le cadre des relations de travail, les exemples de violations des droits des travailleurs ne manquent pas et sont toutes difficiles à prouver. Beaucoup penseront que l'interdiction des *googlelisations* subira le même sort que celles de la non-discrimination, des inégalités homme-femme, de la sous-enchère salariale, du non-paiement des heures supplémentaires, etc.

Cependant, contrairement à toutes les autres violations, une *googlelisation* laisse forcément des traces sur les serveurs de l'entreprise, mais aussi sur ceux des moteurs de recherche et réseaux sociaux.

Or, il ne peut échapper à personne que le droit à l'oubli sur Internet est pour l'instant un vœu pieux[80].

Par conséquent, si un candidat/employé présume avoir été victime d'une *googlelisation* lui ayant causé préjudice, il peut ouvrir une procédure civile et requérir les preuves adéquates. Selon les enjeux, il n'est pas sûr que les juges accèdent facilement à la demande, mais il semble que la justice commence à s'ouvrir davantage à ce genre de requête. Pour s'en convaincre, il suffit de rappeler que le Ministère public genevois a enquêté auprès d'Apple aux USA pour retrouver un SMS[81].

Par exemple, un employé licencié à cause d'une *googlelisation* ou un candidat indûment rejeté de la procédure de sélection peuvent utiliser les règles sur la protection des données pour défendre leurs intérêts et obtenir une réparation pour les dommages subis à cause d'un traitement de données illicite. Bien que pour le candidat, il sera souvent très difficile, voire impossible, de prouver le lien de causalité entre son rejet et la *googlelisation*.

Enfin, n'oublions pas que pour les employés, il est aussi possible d'exiger la cessation d'une surveillance par Internet, même si cela nécessite d'attaquer un employeur en cours d'emploi.

80 http://www.lemonde.fr/technologies/article/2013/10/03/le-droit-a-l-oubli-numerique-inquiete-les-historiens_3489513_651865.html (consulté le 14.01.2014).

81 http://www.20min.ch/ro/news/geneve/story/26480385 (consulté le 14.01.2014).

X. Conclusions

Le devoir de respecter les règles sur la protection des données contraint les recruteurs/employeurs à ne pas recourir à la *googlelisation* des candidats/employés. Il provoque d'ailleurs régulièrement l'étonnement, voire le mécontentement, car il n'est pas rare qu'il remette en cause des traitements de données personnelles établis de longue date[82].

Il faudra sans doute quelques procédures médiatisées, voire des condamnations au paiement de dommages et intérêts non négligeables, pour que s'imposent une prise de conscience et une autodiscipline chez les employeurs.

D'ici là, il sera sûrement difficile de convaincre un recruteur/employeur, seul derrière son écran et son clavier, son smartphone ou sa tablette, de résister à la tentation de vite *googleliser* un candidat/employé pour le protéger d'une atteinte à la personnalité.

Une fois de plus, il est à craindre que nous constaterons à quel point Jean Monnet avait raison en disant que « *Les hommes n'acceptent le changement que dans la nécessité et ils ne voient la nécessité que dans la crise* ».

Néanmoins, les recruteurs/employeurs, qui sont aussi de potentiels candidats/employés, ont-ils tous une image sur le net si irréprochable, que l'adoption de garde-fous dans l'utilisation d'Internet leur restera inconcevable encore longtemps ?

L'ensemble du monde du travail, syndicats d'employés et d'employeurs, devrait s'atteler à régler ce problème avant qu'il n'y ait trop d'atteintes à la personnalité des candidats/employés et de litiges devant la justice, non profitables à tous les acteurs de l'économie.

Gardons à l'esprit pour conclure qu'Albert Einstein a écrit dans les années 1950 « Le progrès technique est comme une hache qu'on aurait mise dans les mains d'un psychopathe ».

[82] Par exemple le contrôle systématique des fiches d'hôtel sur le système d'information Schengen ; la transmission des adresses des participants aux sponsors d'une course à pied populaire ; utilisation des webcams assimilées à des vidéosurveillances.

XI. Bibliographie

AUBERT GABRIEL, La protection des données dans les rapports de travail, in : Journée 1995 de droit du travail et de la sécurité sociale, Zurich 1999, p. 145 ss.

BALZAN MARIE-CHRISTINE, La protection des données des travailleurs dans la due diligence, in : WYLER (édit.), Panorama II en droit du travail, Berne 2012.

BELSER URS, Art. 3, in Datenschutzgesetz, 2e éd., Bâle 2006.

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

DUNAND JEAN-PHILIPPE, in : DUNAND/MAHON (édit.), Commentaire du contrat de travail, Berne 2013.

FLUECKIGER CHRISTIAN, Dopage, santé des sportifs professionnels et protection des données médicales, Genève 2008 (cité : FLUECKIGER, Dopage).

FLUECKIGER CHRISTIAN, Les contrôles antidopage hors compétition sont-ils illicites en Suisse, in : Mélanges en l'honneur de Denis Oswald, Citius, Altius, Fortius, Bâle 2012 (cité : FLUECKIGER, Contrôles antidopage).

GRAMIGNA/MAURER-LAMBROU, Art. 8 et art. 9, in Datenschutzgesetz, 2e éd., Bâle 2006.

JEANDIN NICOLAS, in : PICHONNAZ/FOËX (édit.), Commentaire romand, Code civil I, Bâle 2010.

MAURER-LAMBROU URS, Art. 5, in Datenschutzgesetz, 2e éd., Bâle 2006.

MAURER-LAMBROU/KUNZ, Art. 2, in Datenschutzgesetz, 2e éd., Bâle 2006.

MAURER-LAMBROU/STEINER, Art. 4 et Art. 6, in Datenschutzgesetz, 2e éd., Bâle 2006.

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

RAMPINI CORRADO, Art. 12 et Art. 13, in Datenschutzgesetz, 2e éd., Bâle 2006.

ROSENTHAL/JÖHRI, Handkommentar zum Datenschutzgesetz, Zurich 2008.

RUIZ JEAN-FRANÇOIS, Réussir avec les réseaux sociaux, Paris 2011.

SUBILIA/DUC, Droit du travail – Eléments de droit suisse, Lausanne 2010.

SYLVAIN MÉTILLE[1]

La surveillance électronique des employés

Sommaire

	Page
I. Introduction	100
II. Les exigences légales	101
A. Les lois applicables	101
1. La Loi fédérale sur la protection des données	101
a) Les principes	101
b) Les recommandations du PFPDT	104
2. Les art. 28 ss CC	105
3. La protection de la personnalité du travailleur	105
4. La Loi et l'Ordonnance sur le travail	107
5. Les art. 179 ss CP	108
B. Quelques jurisprudences importantes	109
1. Les balises GPS sur les véhicules d'entreprise	109
2. La caméra cachée dans le local de caisse	110
3. Le logiciel espion installé à l'insu de l'employé	111
4. La surveillance illicite d'un fonctionnaire jurassien	112
5. La surveillance licite d'un fonctionnaire genevois	113
III. L'application et bonnes pratiques	114
A. Les deux questions essentielles	114
1. L'information	114
2. La proportionnalité	116
B. Cas d'application	117
1. La surveillance téléphonique	117
2. La surveillance de l'Internet	120
3. La surveillance du courrier électronique	121
4. La surveillance de l'activité	123
C. Les conséquences d'une surveillance illégale	123
1. L'illégalité de la surveillance	123
2. Le résultat de la surveillance	124
D. La réaction de l'employeur	125

[1] L'auteur remercie chaleureusement Me Nicolas Guyot pour l'aide précieuse apportée dans la mise au point de cet article.

IV. Conclusion 127
V. Bibliographie 128

I. Introduction

Le législateur ayant compris depuis longtemps que la surveillance des travailleurs est de nature à porter une atteinte significative à leur personnalité, plusieurs dispositions légales viennent désormais encadrer et limiter l'activité de l'employeur. Un équilibre délicat doit être trouvé entre les intérêts des différentes parties en présence, soit d'un côté la protection de la sphère privée et de la personnalité du travailleur et de l'autre des intérêts divers et variés comme le respect d'obligations légales, la sécurité, la bonne exécution du travail, etc. Si la facilité de la mise en place d'une surveillance complète d'un réseau informatique ou téléphonique n'est plus à démontrer, cela n'en réduit ni l'atteinte, ni le risque d'abus, bien au contraire. Il est en effet possible, sans connaissances informatiques particulières, d'accéder à un poste à distance, d'enclencher micros et caméras, de recevoir des copies d'écrans et de courriels, de consulter les fichiers journaux, de faire des recherches par mots-clés ou d'être alerté de certains comportements prédéterminés.

Mis à part quelques cas particuliers, l'essentiel des litiges et problèmes rencontrés sont la conséquence d'un manque de connaissance du cadre légal, d'anticipation et de clarification des droits et obligations de chacune des parties. En effet, il est toujours plus facile pour l'employé d'accepter un contrôle (limité) effectué par son employeur lorsqu'il a été préalablement et correctement informé, voire d'en discuter le bien-fondé en dehors de tout cas d'application ; pour l'employeur il est plus facile en cas de problème, de recourir à une procédure préalablement établie et qu'il peut suivre sans avoir, dans l'urgence, à en vérifier la légalité et les conséquences pratiques.

La protection de la sphère privée est garantie par les art. 13 de la Constitution fédérale et 6 de la Convention européenne des droits de l'homme notamment. Ces dispositions sont précisées et complétées par des normes civiles et pénales. Au plan civil, et pour ce qui nous intéresse dans le cadre de cette contribution, il s'agit essentiellement de la Loi fédérale sur la protection des données, des art. 28 ss CC (protection de la personnalité), de l'art. 328 CO (protection de la personnalité du travailleur) complété par l'art. 26 de l'Ordonnance 3 relative à la Loi sur le travail. Au niveau pénal, ce sont principalement les art. 179 ss CP sanctionnant les infractions contre le domaine secret ou privé qui trouveront application.

Cette contribution présente les principales lois applicables et les normes qui les complètent (II. A.) ainsi que quelques décisions judiciaires importantes (II. B.). Deux questions

principales sont ensuite retenues (information et proportionnalité) et quelques cas de surveillance sont appréhendés (III. A. et III. B.). On termine ensuite par les conséquences d'une surveillance illégale (III. C.) et des recommandations pour l'employeur (III. D.). La question de la surveillance des travailleurs en dehors de leur activité, notamment en ce qui concerne l'atteinte à la réputation de l'entreprise sur les réseaux sociaux[2] et la surveillance des candidats et futurs employés[3] dépassent trop largement le cadre de cet article.

II. Les exigences légales

A. Les lois applicables

1. La Loi fédérale sur la protection des données

a) Les principes

La Loi fédérale sur la protection des données (LPD) ne vise pas tant à protéger les données, mais bien plus à protéger la personnalité et les droits fondamentaux des personnes qui font l'objet d'un traitement de données (art. 1 LPD). Elle s'applique aux traitements de données effectués par des personnes privées et des organes fédéraux. Le traitement par des organes cantonaux est réglé par les lois cantonales sur la protection des données, dont le contenu est généralement très similaire à celui de la LPD. Un traitement de données qui viole les principes définis dans la LPD (notamment aux art. 4, 5 et 7 LPD) ou un traitement de données contre la volonté expresse de la personne concernée sont réputés porter atteinte à sa personnalité (art. 12 LPD). Une telle atteinte à la personnalité 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 LPD).

Les grands principes de la protection des données peuvent se résumer comme suit :

– **Le principe de licéité** (art. 4 al. 1 LPD) : tout traitement de données doit être licite aussi bien dans son principe que dans ses modalités et son étendue. L'illicéité peut découler d'une norme de la LPD, mais également d'une norme impérative provenant d'un autre texte de loi (par exemple les art. 47 LB, 320 ss CP, 179 ss CP, etc.)[4].

2 Voir dans le présent ouvrage la contribution de AUBERT CAROLE/DELLEY RÉGINE, p. 148 ss.
3 Voir dans le présent ouvrage la contribution de FLÜCKIGER CHRISTIAN, p. 73 ss.
4 MEIER, p. 260-263 ; ROSENTHAL/JÖHRI, p. 78-81.

- **Le principe de bonne foi** (art. 4 al. 2 LPD) : ce principe général de l'Ordre juridique suisse s'applique évidemment aussi en matière de protection des données. En l'absence de dispositions particulières visant les failles de sécurité, on pourrait dans certains cas déduire du principe de la bonne foi une obligation pour le responsable du traitement d'informer les personnes concernées en cas de perte de données ou de perte de maîtrise sur ces données[5].
- **Le principe de proportionnalité** (art. 4 al. 2 LPD) : il découle de ce principe que l'on ne doit collecter et traiter que les données qui sont aptes et objectivement nécessaires pour atteindre le but visé, dans le cadre d'un traitement qui demeure dans un rapport raisonnable entre le résultat recherché et le moyen utilisé, tout en préservant le plus possible les droits des personnes concernées. Cela implique une pesée d'intérêts entre le but du traitement des données et l'atteinte portée à la personnalité des personnes concernées. Le principe de proportionnalité est souvent violé dans la pratique qu'il s'agisse de la quantité de données collectées, de la durée pendant laquelle elles sont conservées, du nombre de personnes qui y ont accès, ou simplement de l'existence d'autres moyens permettant d'obtenir les mêmes résultats, sans avoir à traiter de données personnelles[6].
- **Le principe de reconnaissabilité** (art. 4 al. 4 LPD) : contrairement à ce qui prévaut dans d'autres pays, le droit suisse n'exige pas qu'un traitement de données soit systématiquement autorisé par le consentement de la personne concernée sur la base d'une information expresse. Au contraire, c'est une approche pragmatique et praticable qui a été retenue par le législateur suisse. Le traitement de données doit être reconnaissable par la personne concernée, qui peut alors s'opposer au traitement. D'une certaine manière, le consentement est alors présumé. La reconnaissabilité doit néanmoins recouvrir la collecte (principe, étendue, type de données collectées), le but dans lequel les données sont collectées, et seront traitées, ainsi que l'identité du maître du fichier. Dans le cas du traitement de données sensibles ou de profils de la personnalité, il existe un devoir d'information (art. 14 LPD)[7].
- **Le principe de finalité** (art. 4 al. 3 LPD) : les données ne peuvent pas être traitées dans un but autre que celui qui était reconnaissable ou communiqué lors de leur collecte. Un sous-traitant est également lié par le but initial annoncé. Si un traitement différent est envisagé, une information complémentaire est nécessaire et la personne visée doit avoir la possibilité de s'y opposer. Cela implique aussi que l'on ne peut pas collecter des données uniquement dans le but de les avoir à disposition pour le cas où

5 MEIER, p. 263-267.
6 MEIER, p. 267-274 ; ROSENTHAL/JÖHRI, p. 83-89.
7 MEIER, p. 274-281 ; ROSENTHAL/JÖHRI, p. 96-103.

elles pourraient éventuellement être utiles (cela violerait évidemment aussi le principe de proportionnalité)[8].

- **Le principe d'exactitude** (art. 5 al. 1 LPD) : les données traitées doivent être correctes et les mesures appropriées prises pour effacer ou rectifier les données inexactes ou incomplètes. Chacun a le droit d'obtenir la rectification des données erronées ou incomplètes. Le maître du fichier doit également s'assurer que les données qu'il traite sont toujours actuelles et correctes[9].
- **Le principe de sécurité** (art. 7 al. 1 LPD) : les données personnelles doivent être protégées contre tout traitement non autorisé par des mesures organisationnelles et techniques appropriées. Les détails sont réglés dans l'Ordonnance relative à la Loi fédérale sur la protection des données (OLPD), ainsi qu'un guide du Préposé fédéral à la protection des données et à la transparence « mesures techniques et organisationnelles : guide »[10]. Il s'agit notamment d'assurer la confidentialité, la disponibilité et l'intégrité des données[11].

En résumé, « les données personnelles peuvent être collectées uniquement de manière légale. Leur traitement est régi par le principe de la bonne foi et doit être effectué selon les dispositions de la Loi sur la protection des données et de l'Ordonnance y afférente. Le principe de la proportionnalité doit toujours être respecté. Il ne peut être traité que des données qui sont en relation avec le but du traitement. Celles-ci doivent en outre être détruites dans un délai le plus bref possible, défini à l'avance. L'accès aux données personnelles traitées [fichier] doit faire l'objet d'une règlementation. Il doit être limité aux personnes qui sont autorisées à avoir accès à ces données »[12].

Ces principes sont applicables à la surveillance électronique des travailleurs. « Lors de l'utilisation de système de surveillance ou de contrôle, il faut toujours veiller à garantir la protection de la personnalité des collaboratrices et des collaborateurs. Les personnes concernées doivent être informées au préalable sur la nature, le but et la finalité du traitement de données. Si possible, on élaborera un règlement d'utilisation interne à l'entreprise qui informe de manière transparente les collaboratrices et collaborateurs sur leurs droits et obligations lors de l'utilisation de systèmes de surveillance ou de contrôle […]. L'employeur consciencieux doit cependant toujours se rappeler qu'une utilisation de tels systèmes sans annonce préalable éveille la méfiance. Néanmoins, un contrôle raisonnable et concevable peut sans autre être justifié. Un contrôle est notamment consi-

8 MEIER, p. 281-286 ; ROSENTHAL/JÖHRI, p. 89-96.
9 MEIER, p. 287-297 ; ROSENTHAL/JÖHRI, p. 124-128.
10 Disponible sur le site : www.leprepose.ch (consulté le 1er novembre 2013).
11 MEIER, p. 297-316 ; ROSENTHAL/JÖHRI, p. 176-185.
12 PFPDT, 20e rapport, p. 71.

déré comme étant raisonnable et concevable lorsque la transparence est de mise et que l'on ne découvre pas avec surprise un "espionnage". »[13].

b) Les recommandations du PFPDT

Le Préposé fédéral à la protection des données et à la transparence (PFPDT) a publié plusieurs documents, en particulier des explications sur la surveillance téléphonique sur le lieu du travail, un 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, et des explications sur la vidéosurveillance sur le lieu de travail[14]. Le Tribunal fédéral s'est récemment référé aux modalités préconisées par le PFPDT en matière de surveillance pour délimiter ce qui est admissible de ce qui est excessif, donnant de fait une force particulière à ces recommandations[15].

Les explications sur la vidéosurveillance sur le lieu de travail rappellent les conditions habituelles à la mise en place d'un système de vidéosurveillance, et ajoutent le fait que les travailleurs ou leurs représentants ont un droit de regard avant la mise en place d'un système de vidéosurveillance. Les explications conseillent également d'utiliser les technologies permettant de protéger les données comme des filtres qui brouillent les visages filmés en temps réel (techniques de floutage, les images étant seulement décryptées par les personnes autorisées en cas de nécessité). Les explications envisagent ensuite les différentes finalités possibles et présentent une série d'exemples particuliers (vidéosurveillance sur des chantiers, dans les grands magasins et les banques, dans un centre de tri postal, dans un atelier d'orfèvre et dans un kiosque).

Les explications sur la surveillance téléphonique sur le lieu de travail reprennent des conditions similaires et s'attachent à la distinction entre les appels privés et les appels professionnels. Les problèmes particuliers soulevés par les appareils mains libres munis d'un haut-parleur, l'affichage du numéro de l'appelant, la liste des appelants, l'annonce directe par haut-parleur et les conférences téléphoniques sont également appréhendés.

Le guide relatif à la surveillance de l'utilisation d'Internet et du courrier électronique au lieu de travail est le plus complet. Il rappelle en détails les principes à respecter ainsi que les différentes analyses possibles (analyse anonyme, analyse pseudonyme et analyse nominale). Il contient également un règlement type de surveillance de l'utilisation d'Internet et du courrier électronique au lieu de travail.

---

13 PFPDT, 20e rapport, p. 71-72.

14 Tous ces documents sont disponibles sur le site www.leprepose.ch (consulté le 1er novembre 2013).

15 ATF 139 II 7, JdT 2013 II 188 (rés.), SJ 2013 I 177 (rés.). Voir p. 111 ci-après. Voir également COSTA.

2. Les art. 28 ss CC

La personnalité est protégée de manière générale contre les atteintes illicites par les art. 28 ss CC[16]. Une atteinte n'est pas illicite lorsqu'elle est justifiée par le consentement de la victime, par un intérêt privé ou public prépondérant ou par la loi (art. 28 al. 2 CC). Contrairement aux normes protectrices de droit constitutionnel, qui tendent à prémunir le particulier contre les atteintes illicites émanant de l'Etat et de ses organes, la protection conférée par les art. 28 ss CC déploie ses effets entre les particuliers[17].

Les art. 28 ss CC protègent les différentes composantes du droit de la personnalité telles que les droits de la personne physique (droit à la vie, droit à l'intégrité corporelle physique et psychique, droit à la liberté de mouvement), les droits de la personnalité affective (droit aux relations avec les proches) et les droits de la personne sociale (droit au nom, droit au respect de la vie privée, droit au respect de l'honneur, droit à l'image)[18].

Les art. 28 ss CC protègent également la personne contre la divulgation à des tiers de données la concernant et relevant de sa vie privée[19]. L'art. 28 CC concrétise et renforce la protection de la personnalité et des droits fondamentaux dans le contexte du traitement de données personnelles[20]. La LPD renvoie d'ailleurs expressément, s'agissant des actions, aux art. 28 ss CC (art. 15 LPD)[21].

L'art. 28*a* CC décrit les actions à disposition de la victime, à savoir les moyens défensifs (action en interdiction de l'atteinte, action en cessation de l'atteinte et action en constatation du caractère illicite). La communication ou la publication du jugement peut aussi être obtenue. Les moyens réparateurs sont mentionnés à l'art. 28*a* al. 3 CC qui réserve les actions en dommages-intérêts et en réparation du tort moral, ainsi que la remise de gain selon les dispositions sur la gestion d'affaires (art. 41, 49, et 423 CO).

3. La protection de la personnalité du travailleur

L'art. 328 CO régit le devoir de l'employeur de protéger la personnalité de ses employés en concrétisant, dans le cadre de la relation de travail, les principes généraux des art. 28 ss CC. Cette norme est relativement impérative, c'est-à-dire qu'il ne peut pas y être dérogé au détriment du travailleur (art. 362 CO). En vertu de l'art. 328 al. 1 CO, l'employeur doit protéger et respecter la personnalité du travailleur. Ce principe revêt

16 MEILI, N 32 et 33 ad art. 28 CC.
17 JEANDIN, N 7 ad art. 28 CC.
18 JEANDIN, N 23 à 50 ad art. 28 CC ; MEILI, N 16 à 31 ad art. 28 CC.
19 JEANDIN, N 51 ad art. 28 CC.
20 JEANDIN, N 51 et 52 ad art. 28 CC.
21 MEIER, p. 563-591.

une importance particulière dans les rapports de travail en raison du rapport de subordination du travailleur à l'égard de l'employeur. Il constitue le pendant du devoir de fidélité du travailleur résultant de l'art. 321*a* CO. L'employeur répond également des actes de ses organes et de ses auxiliaires[22]. Certaines conventions collectives de travail contiennent des dispositions complémentaires[23].

L'employeur doit non seulement respecter la personnalité du travailleur, mais aussi la protéger. Il doit donc autant s'abstenir de porter atteinte au droit de la personnalité de ses employés que prendre des mesures adéquates pour empêcher qu'ils ne subissent une atteinte.

L'art. 328*b* CO rappelle 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. Cette disposition légale fait le lien avec la LPD et concrétise notamment les principes de proportionnalité et de finalité[24].

Comme dans n'importe quel cas de traitement de données, l'auteur du traitement peut faire valoir des motifs justificatifs. Dans le cadre de la relation de travail, il est rare de pouvoir obtenir un consentement valable du travailleur à une atteinte à sa personnalité. En effet, pour être valable un consentement doit être libre et éclairé. Le déséquilibre structurel qui existe entre l'employeur et l'employé (du fait du lien de subordination inhérent au contrat de travail) amène à poser des exigences plus strictes en matière de liberté du consentement. Plus l'acte auquel le travailleur consent est éloigné du cadre de l'art. 328*b* CO, plus il sera difficile d'admettre la validité du consentement. Néanmoins, si l'acte est dans l'intérêt premier du travailleur, on admettra alors plus facilement que le consentement peut être valablement donné[25].

Les autres motifs justificatifs, en particulier l'intérêt privé prépondérant de l'employeur, peuvent évidemment être réalisés et rendre licite une atteinte portée à la personnalité de l'employé[26]. On pense notamment à des motifs de sécurité, de contrôles de qualité, de prévention des accidents, ou de preuves en cas de litige ultérieur. L'application du principe de proportionnalité implique pour l'employeur l'obligation de choisir la mesure la moins intrusive parmi toutes celles possibles[27].

---

22 DUNAND, N 1 à 103 ad art. 328 CO.
23 AUBERT, p. 146 et 167.
24 DUNAND, N 4 ad art. 328*b* CO ; MEIER, p. 650.
25 DUNAND, N 32 ad art. 328*b* CO ; MEIER, p. 327-328 et 657-658.
26 WYLER, p. 303 ; SUBILIA/DUC, p. 344-345.
27 WYLER, p. 303.

4. La Loi et l'Ordonnance sur le travail

La Loi sur le travail (LTr) prévoit à son art. 6 al. 1 que 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, pour protéger la santé des travailleurs. Il doit en outre prendre toutes les mesures nécessaires pour protéger l'intégrité personnelle des travailleurs. Se basant sur cette disposition, le Conseil fédéral a adopté l'Ordonnance 3 relative à la Loi sur le travail (OLT 3), dont l'art. 26 dispose 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. Lorsque des systèmes de surveillance ou de contrôle 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.

Alors que le premier alinéa de cette disposition prévoit une interdiction claire de tout système destiné à surveiller le comportement des travailleurs, le second alinéa autorise le recours à un système de surveillance pour d'autres raisons. Parmi ces autres raisons, on relèvera les impératifs liés à la prévention des accidents, à la protection ou à la sécurité des personnes et des biens, ainsi que des motifs tenant à l'organisation ou à la planification du travail ou encore des objectifs de contrôle du travail (qualité des prestations et du rendement)[28]. Pour examiner si un système de surveillance est admissible, il faut s'attacher au but de la surveillance et non à ses effets[29].

Cet article concrétise à la fois le besoin de l'employeur de pouvoir exercer un certain contrôle sur l'activité et les prestations de son personnel, ce qui correspond à la nature même des relations de travail qui sont caractérisées par un lien de subordination, et l'atteinte illicite à la personnalité que constituent des mesures de surveillance portant uniquement sur le comportement des travailleurs[30].

Le SECO a publié en mars 2013 un nouveau Commentaire de l'Ordonnance 3 relative à la Loi sur le travail qui rappelle notamment les obligations et principes contenus dans la LPD et propose un modèle de planification et de décision concernant la mise en place d'un système de surveillance et de contrôle technique à l'intention des employeurs, des travailleurs et des inspecteurs[31]. Le commentaire met l'accent sur le respect du principe de proportionnalité[32].

---

28 MEIER, p. 687-688.
29 ATF 130 II 425 (voir *infra* chap. B.1).
30 DUNAND, N 85-86 ad art. 328*b* CO, et TESTER p. 3-4.
31 Disponible sur le site www.seco.admin.ch (consulté le 1er novembre 2013).
32 SUBILIA/DUC, p. 347-348.

5. Les art. 179 ss CP

L'art. 321ter CP sanctionne la violation du secret des postes et les télécommunications. Il ne s'applique cependant qu'aux personnes astreintes à ce secret, qu'elles soient employées de manière fixe ou temporaire, par une entreprise privée ou publique. Est déterminant le fait que l'activité professionnelle donne accès à des données couvertes par le secret des postes et les télécommunications[33].

Les art. 179 ss CP visent les infractions contre le domaine secret ou le domaine privé, notamment l'ouverture de la correspondance, l'enregistrement de conversations téléphoniques ou la prise de vue. L'art. 179 CP sanctionne la violation de secrets privés, soit l'acquisition et l'exploitation d'informations contenues dans un pli ou un colis fermé. Si la fermeture ne doit pas opposer une résistance sérieuse, elle doit néanmoins permettre de déduire de bonne foi que l'expéditeur n'a pas voulu que le contenu soit accessible à n'importe qui [34]. Le courriel est souvent comparable à une carte postale, qui n'est pas protégée par l'art. 179 CP car une fermeture empêchant que le contenu ne soit accessible à quiconque fait défaut[35]. En revanche, si une mesure est prise par l'expéditeur, par exemple sous la forme d'un cryptage, on doit admettre que le courriel n'est pas librement accessible. L'art. 179bis CP assure une protection similaire pour les échanges oraux.

Quant à l'art. 179quater CP, il sanctionne la violation du domaine secret ou du domaine privé au moyen d'un appareil de prises de vue. Sont ainsi protégés les faits relevant du domaine secret ou du domaine privé et qui ne sont pas accessibles à tout le monde. Le législateur a notamment voulu protéger la sphère personnelle et la vie en famille. Comme en matière d'écoute, sont punies l'observation avec un appareil de prise de vues d'une part et la fixation sur un porteur d'images d'autre part. L'observation à l'œil nu, avec des jumelles, à travers une glace sans tain, ou au moyen d'un autre appareil qui améliore les possibilités de vue mais ne permet pas l'enregistrement de l'image n'est pas sanctionnée par cette disposition légale[36].

33 CORBOZ, Vol. II, p. 786-791.
34 CORBOZ, Vol. I, p. 633.
35 CORBOZ, Vol. I, p. 634 ; MONNIER, p. 142.
36 ATF 117 IV 31.

B. Quelques jurisprudences importantes

1. Les balises GPS sur les véhicules d'entreprise[37]

Le Tribunal fédéral devait se prononcer sur la légalité de l'installation de balises GPS par l'employeur sur les véhicules d'entreprise utilisés par les employés chargés de vendre et assurer le service après-vente et la maintenance d'extincteurs incendie. Ces véhicules, que les employés utilisaient trois à quatre heures par jour, étaient réservés exclusivement à usage professionnel.

Le Tribunal fédéral a d'abord repris les principes des art. 328 ss CO et 26 OLT 3, et en particulier le fait que c'est moins le type de surveillance ou ses effets comme tels qui vont déterminer si un système est admissible ou non, mais surtout les motifs qui ont prévalu à sa mise en place ou les buts que poursuit son utilisation. Au titre des autres raisons susceptibles de justifier le recours à un système de surveillance, le Tribunal fédéral mentionne d'une part les impératifs liés à la prévention des accidents ou la protection ou la sécurité des personnes et des biens, et d'autre part des motifs tenant à l'organisation ou à la planification du travail selon les circonstances et le type d'activité considérés. A titre d'exemple, le Tribunal fédéral cite des sociétés qui offrent des services financiers en ligne et qui pour des motifs de preuves doivent pouvoir enregistrer les conversations téléphoniques entre leurs collaborateurs et les clients, ou des agences de sécurité, de taxis ou de transports qui requièrent, afin de rationaliser le travail et d'améliorer la qualité des prestations, que l'employeur ait la possibilité de localiser en tout temps et aussi vite que possible la position de chacun des véhicules en service, etc.

Le Tribunal fédéral souligne qu'il est dans la nature même des relations de travail que l'employeur puisse exercer un certain contrôle sur l'activité et les prestations de son personnel. La faculté qui lui est reconnue et parfois l'obligation d'établir des directives générales ou de donner des instructions particulières sur la manière d'exécuter le travail ou de se conduire dans l'entreprise a pour corollaire qu'il doit pouvoir s'assurer que ses consignes sont correctement suivies par les travailleurs. L'employeur est ainsi 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.

Dans le cas d'espèce, le Tribunal fédéral a retenu que les véhicules d'entreprise ne pouvaient pas être utilisés à des fins privées et que la localisation en temps réel des véhicules n'était possible que sur requête à une centrale de télésurveillance. La surveillance induite

[37] ATF 130 II 425, X. SA c/ Office cantonal de l'inspection et des relations du travail, du 13 juillet 2004.

par le système de localisation est de plus médiate, car elle ne porte pas sur les collaborateurs eux-mêmes, mais sur les véhicules qu'ils utilisent pour visiter les clients dont ils ont la charge. Elle n'appréhende qu'un aspect de leur comportement, à savoir les déplacements qu'ils effectuent durant la journée de travail, ce qui dans le cas d'espèce représente trois à quatre heures par jour. Ainsi, la surveillance n'étant qu'indirecte, partielle et intermittente, l'atteinte qu'elle cause apparaît proportionnée au but légitime visé par l'employeur, qui est de connaître l'emploi du temps journalier de ses collaborateurs afin de prévenir les abus et de s'assurer qu'ils accomplissent correctement leurs tâches, en particulier qu'ils respectent les horaires de travail et qu'ils effectuent bien les visites qu'ils sont tenus de faire.

Le Tribunal fédéral poursuit que cette surveillance n'est pas très différente de celle que l'on peut trouver dans une entreprise équipée d'une machine à timbrer, où les employés doivent pointer à chaque fois qu'ils entrent dans l'entreprise ou qu'ils la quittent, y compris lorsqu'ils s'absentent un court instant durant la journée, en indiquant, le cas échéant, le motif de leur absence. En revanche, si le système de localisation permettait de suivre de manière continue et en temps réel le trajet emprunté par chaque véhicule, il pourrait constituer un moyen de surveillance disproportionné par rapport au but poursuivi. L'intensité de l'atteinte à la santé, à la personnalité et à la liberté de mouvement des travailleurs ne serait en effet pas la même s'ils sont soumis de manière continue et en temps réel à la surveillance de leur employeur ou si seul un contrôle *a posteriori* est effectué, en fin de journée, sous la forme d'une comparaison entre le contenu des rapports d'activités et les informations ponctuelles fournies par le système de localisation.

2. La caméra cachée dans le local de caisse[38]

La Cour de droit pénal devait se prononcer sur la légalité de preuves issues d'une caméra de surveillance installée sur le lieu de travail. La caméra était installée à l'insu des travailleurs dans le local de caisse d'un magasin de montres et de joaillerie. Les employés ne se trouvent que sporadiquement dans ce local et pendant de courtes durées, en particulier lorsqu'ils doivent y déposer ou y prélever des espèces. La vidéo enregistrant principalement la caisse et les travailleurs ne s'y trouvant que sporadiquement et pendant un bref moment, la Cour a considéré qu'une telle surveillance vidéo n'était pas de nature à porter une atteinte à la santé et au bien-être des travailleurs. Un système de surveillance peut être permis même s'il sert principalement à la surveillance ciblée du comportement des travailleurs sur leur lieu de travail, si les travailleurs ne sont enregistrés que pendant peu de temps et à des occasions particulières.

38 TF 6B_536/2009, A. SA c. Ministère public du canton de Zurich, du 12 novembre 2009. Voir également le commentaire de TESTER, p. 10-12.

Si l'installation avait aussi pour but la prévention d'infractions pénales par des tiers, son but principal était la surveillance des travailleurs. Considérant que des sommes en espèces d'un montant considérable peuvent se trouver dans le local de la caisse du magasin, la Cour retient que le propriétaire a un intérêt tout aussi considérable à la surveillance, qui reste proportionnée vu que les employés n'y sont que de manière limitée.

La mesure de surveillance n'a donc pas été considérée comme illicite et les preuves n'ont pas été écartées. Si l'installation de surveillance avait visé de manière continue un employé travaillant au comptoir, le résultat aurait certainement été différent. L'atteinte aurait été d'une part largement supérieure, et d'autre part l'intérêt que peut faire valoir l'employeur pour surveiller un local de caisse à l'arrière d'une bijouterie n'est à l'évidence pas le même que celui d'un comptoir ou de la caisse enregistreuse d'un supermarché.

3. Le logiciel espion installé à l'insu de l'employé[39]

Dans cette affaire, le Tribunal fédéral devait se prononcer pour la première fois sur la licéité de l'usage d'un logiciel espion à l'insu de l'employé. Le consortium de la protection civile tessinois soupçonnait un de ses employés d'utiliser de manière abusive et à des fins personnelles les ressources informatiques mises à sa disposition. L'employeur a ainsi fait installer à l'insu de l'employé un logiciel espion qui a révélé, durant trois mois, que l'employé avait consacré une part importante de son temps de travail à des activités privées ou à tout le moins étrangères à son activité professionnelle. Grâce à des copies d'écran effectuées à des intervalles réguliers, le contrôle a permis de prendre connaissance du contenu des pages Internet consultées et des messages électroniques, y compris des informations privées comme des opérations bancaires en relation avec la fonction de membre du conseil municipal de l'employé. L'employeur a conduit une enquête administrative puis a licencié avec effet immédiat cet employé.

Le Tribunal fédéral a retenu que l'utilisation clandestine d'un logiciel espion était illicite et constituait une mesure prohibée par l'art. 26 al. 1 OLT 3 car elle est assimilable à un système de contrôle destiné essentiellement à surveiller le comportement du travailleur. Cette mesure était au surplus clairement disproportionnée.

Si l'employeur a un intérêt légitime à lutter contre les abus, il peut y parvenir à l'aide de moyens moins invasifs comme le blocage à titre préventif de certains sites Internet, ou une analyse conformément aux modalités indiquées par le Préposé fédéral à la protection des données et à la transparence, modalités auxquelles le Tribunal fédéral renvoie ex-

39 ATF 139 II 7, JdT 2013 II 188 (rés.), SJ 2013 I 177 (rés.), Consortium de la protection civile Z. c. X., du 17 janvier 2013.

pressément. L'employeur aurait également pu, par des mesures moins incisives, assurer la protection de son droit d'éviter des abus de la part de son employé, en procédant à l'examen de fichiers journaux, en rappelant son employé à l'ordre et en lui donnant l'occasion de modifier son comportement. Les informations obtenues ont donc été considérées comme illicites et ne pouvaient pas être utilisées comme preuves du licenciement. En l'absence d'autres fondements, le licenciement qui se fondait sur un rapport de droit public a été annulé.

4. La surveillance illicite d'un fonctionnaire jurassien

Dans un arrêt de la Cour administrative du Tribunal cantonal jurassien du 25 février 2013[40], la Cour devait se prononcer sur le recours d'un fonctionnaire qui avait été déclassé suite à la consultation de sites non professionnels. A fin 2008, le Service de l'informatique du canton du Jura avait procédé à des analyses techniques étendues suite à la constatation de lenteurs dans l'accès à Internet. Ce service s'était également appuyé sur les services d'une entreprise externe pour analyser des fichiers journaux des postes utilisés par des fonctionnaires et magistrats, après avoir obtenu de ceux-ci qu'ils permettent au service informatique d'accéder à leurs ordinateurs, en prétextant faussement procéder à une opération de maintenance. Les informations ont ensuite été transmises au Gouvernement et au Conseil de la magistrature, qui ont prononcé diverses sanctions.

Dans le cas d'espèce, un fonctionnaire contestait le déclassement dont il faisait l'objet au motif que les preuves recueillies étaient illicites. La Commission cantonale jurassienne de la protection des données avait précédemment constaté que la récolte de ces données était illégale et qu'elles devaient être détruites[41]. Les données concernant d'autres fonctionnaires, recueillies dans les mêmes conditions, avaient déjà été utilisées pour prononcer des sanctions qui n'avaient pas été contestées et étaient donc entrées en force.

La Cour administrative a retenu que la surveillance n'avait pas été autorisée ni prévue par la loi et que les preuves recueillies étaient illicites. Procédant à une pesée d'intérêts, la Cour a conclu que l'intérêt du recourant à bénéficier d'une instruction conforme au droit et respectant la protection de la sphère privée, doit primer sur l'intérêt de l'autorité disciplinaire à l'établissement de la vérité, et cela d'autant plus que l'atteinte à la sphère privée est importante alors que l'usage abusif d'Internet est en général une faute d'importance mineure. Les preuves illicites ont donc été déclarées inexploitables, de même que les déclarations du recourant qui avaient suivi ces analyses illicites. Faute de

40 Arrêt de la Cour administrative du Tribunal cantonal jurassien du 25 février 2013, X. c. le Gouvernement de la République et Canton du Jura (ADM 92/2009).

41 Décision de la Commission cantonale jurassienne de la protection des données à caractère personnel du 29 mars 2012.

preuves exploitables, aucun usage abusif ne pouvait être constaté et aucune sanction n'était justifiée.

5. La surveillance licite d'un fonctionnaire genevois

Dans un arrêt de la Cour de justice du canton de Genève du 28 mai 2003[42], la Cour devait se prononcer sur le recours d'un cadre de la Ville, qui avait été licencié avec effet immédiat pour avoir notamment visionné des vidéos à caractère pornographique sur son ordinateur. L'employé avait préalablement été informé de la Directive relative à l'utilisation des systèmes d'information et de communication, qui prévoyait que l'utilisation des systèmes était limitée aux besoins professionnels, que leur utilisation à des fins privées était tolérée de manière occasionnelle et qu'en cas de soupçons de violation de la Directive, une surveillance individualisée pouvait être effectuée pour une durée limitée.

Dans le cas d'espèce, il y avait de forts soupçons de consultations importantes de sites pornographiques pendant le temps de travail. Une surveillance a donc été ordonnée dans les formes prévues par la Directive et autorisée par l'autorité compétente. Elle s'est déroulée en deux temps et sur des périodes limitées, la première confirmant la consultation de sites pornographiques, alors que la seconde a permis de reconstituer les fichiers effacés sur le poste de travail. Le disque privé n'a pas été examiné. Dans ces conditions, la Cour a retenu que les moyens utilisés pour procéder à ces surveillances, notamment l'analyse de processus lancée sur le poste de travail de l'intéressé, des fichiers journaux relatifs à la navigation, de l'anti-virus, du disque dur, des fichiers effacés et des fichiers du lecteur multimédias respectait pleinement l'art. 26 OLT 3 et le principe de proportionnalité. La surveillance était donc licite et les moyens de preuves qui en résultent pouvaient être utilisés. Le licenciement a donc été confirmé.

Ce cas diffère principalement du précédent sur les questions de légalité et de proportionnalité. Premièrement, le Jura ne disposait pas, à l'époque des faits, d'une directive ou d'un règlement suffisamment précis pour permettre une telle mesure de surveillance. La compétence du service informatique seul n'était pas clairement établie non plus. Contrairement à ce qui vaut pour un employeur privé, l'Etat ne peut en principe pas se réfugier derrière un intérêt prépondérant mais il a besoin d'une base légale pour pouvoir porter atteinte à la personnalité d'un employé. Deuxièmement, l'atteinte était disproportionnée : il était par exemple possible de résoudre le problème de surcharge du réseau en bloquant seulement certains sites et les informations recueillies dépassaient largement ce qui était

42 Arrêt de la Cour de justice du canton de Genève, X. c. Ville de Genève, du 28 mai 2003 (ATA/329/2013).

nécessaire pour démontrer un abus (si tel était le but). La méthode utilisée pour accéder à distance de certains postes de travail, en particulier en demandant l'accord de l'employé de procéder à ce qui était annoncé comme une opération de maintenance, posait également problème.

III. L'application et bonnes pratiques

A. Les deux questions essentielles

1. L'information

De manière pragmatique, tout employeur qui envisage ou exécute une surveillance de ses employés et qui ne veut pas procéder à un examen légal complet devrait au moins vérifier s'il a bien informé les employés et les autres personnes visées, et si l'atteinte portée est proportionnée par rapport aux buts (légitimes) visés. Ces deux questions, auxquelles on peut ajouter la recherche d'éventuels motifs justificatifs, ressortent d'une manière ou d'une autre des différentes normes légales, des recommandations du SECO et du PFPDT, ainsi que de la jurisprudence civile, administrative et pénale.

Toute mesure de surveillance devrait être annoncée préalablement. Cela ne signifie pas que l'on va toujours indiquer au travailleur le moment précis auquel on le surveille, mais qu'une information complète doit lui être donnée sur les conditions, modalités et buts de la surveillance.

La législation sur le travail requiert une information préalable et détaillée qui doit couvrir le type et le but du traitement des données[43]. L'employeur n'a par exemple pas le droit de procéder à l'analyse de fichiers journaux (données secondaires) sans avoir préalablement édicté un règlement ou avoir informé le personnel[44]. Dans le cas de la surveillance téléphonique, l'information doit indiquer le système de surveillance utilisé, son mode opératoire, la possibilité d'effectuer des contrôles, les droits d'accès, le contenu et la durée de conservation des données journalisées[45].

Les travailleurs disposent en outre d'un droit à l'information et à la consultation, ce qui leur donne le droit de faire des propositions avant la mise en place d'une surveillance et de participer à d'éventuelles investigations et visites de l'entreprise faites par les autori-

43 SECO, p. 6.
44 PFPDT, Guide, p. 7.
45 PFPDT, Explications surveillance téléphonique, p. 2.

tés[46]. Au regard de la LPD, on peut se demander si une information expresse doit être donnée (considérant que les données personnelles traitées sont des données sensibles ou des profils de la personnalité au sens de l'art. 3 LPD) ou si le traitement des données et sa finalité doivent seulement être reconnaissables[47]. La réponse dépendra évidemment des situations. L'exigence d'information découlant de la LPD (contrairement à celle découlant du droit du travail) ne s'applique pas seulement aux travailleurs, mais également à toute personne dont les données sont traitées (clients, visiteurs, interlocuteurs, etc.).

Au regard des articles 179 ss du CP, un enregistrement à l'insu de l'employé aura généralement lieu sans droit. En effet, un des éléments constitutifs de ces infractions est précisément l'absence de consentement de la ou des personnes visées. Or il est impossible de consentir valablement à quelque chose que l'on ignore et l'information est bien une condition préalable du consentement. Cette interprétation ressort également des travaux préparatoires. Le projet exigeait en effet comme condition de punissabilité de l'art. 179ter CP que l'enregistrement soit « clandestin »[48]. Le Conseil national n'a pas retenu cette proposition estimant que le caractère secret de l'enregistrement résultait déjà « en partie » de l'absence de consentement[49].

L'information ne doit pas obligatoirement être écrite, mais cela est vivement recommandé pour des questions de preuves notamment. Dans le cadre d'une procédure, ce serait à l'employeur de démontrer que les employés ont été correctement et complètement informés. Au surplus, si cette information devait conditionner un éventuel consentement de l'employeur, il est d'autant plus important que ce dernier ait eu la possibilité de recevoir les informations de manière complète, mais aussi de les examiner et de demander des informations supplémentaires.

On ne peut donc que recommander à chaque employeur d'adopter un règlement qui permette d'informer clairement et complètement les travailleurs non seulement des mesures de surveillance qui peuvent être ordonnées (et les conditions auxquelles elles peuvent l'être), mais également de l'usage privé admis au sein de l'entreprise (utilisation de l'infrastructure de l'entreprise à titre privé, utilisation pendant le temps et sur le lieu de travail d'outils privés tels que téléphone ou ordinateur personnel, …), la procédure à suivre pour mettre en place une surveillance et l'exploitation possible de son résultat, ainsi que les sanctions pouvant être prononcées en cas de violation du règlement. Le

46 Art. 5 et 6 OLT 3 ; SECO, p. 7.
47 Art. 4 al. 4 LPD.
48 Message du CF concernant le renforcement de la protection pénale du domaine personnel secret du 21 février 1968, FF 1968 I 609, p. 619.
49 BOCN, 1968, p. 342 ; STRATENWERTH/JENNY/BOMMER, p. 274.

PFPDT propose un règlement-type de surveillance de l'utilisation d'Internet et du courrier électronique au lieu de travail[50]. L'employeur serait aussi bien avisé d'intégrer dans ce règlement les aspects liés au comportement en ligne (réseaux sociaux, sites Internet, etc.), à l'utilisation du nom et de l'image de l'entreprise, etc.

L'absence d'information préalable du travailleur n'est pas systématiquement une cause d'illégalité de la mesure de surveillance. Il peut exister, dans des cas particuliers, des motifs justificatifs suffisants qui permettent de corriger l'absence d'information, mais cela ne peut pas être la règle.

Dans le cas où une surveillance n'est mise en place que dans un but précis et après la découverte de forts soupçons d'abus, de violation de directives de l'employeur ou d'atteinte aux intérêts de ce dernier, une mesure de surveillance devrait pouvoir être mise en place sans que la personne n'en soit informée préalablement. Lorsqu'il soupçonne de manière fondée un employé d'avoir commis ou de s'apprêter à commettre une infraction pénale, l'employeur pourra se fonder sur un intérêt prépondérant privé pour ne pas informer préalablement la personne mise en cause des mesures de surveillance qu'il entend prendre à son égard[51].

On admettra la plupart du temps que des données peuvent être sauvées à titre de preuves sans en informer l'employé (dans le but évident qu'il ne les détruise pas ou ne les modifie pas), en revanche leur exploitation ne devrait avoir lieu qu'après que l'employé en ait été informé. Une information complète devrait néanmoins être transmise dès qu'il n'y a plus de motifs justifiant de conserver la surveillance secrète. Si des informations sont disponibles ou ont été enregistrées à l'insu de l'employé, ce dernier devrait au moins être informé avant qu'elles ne soient exploitées.

2. La proportionnalité

Le principe de la proportionnalité doit être respecté tant dans le choix de la mesure de surveillance que dans son utilisation et dans l'exploitation finale de ces résultats. 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. C'est donc au niveau du principe de proportionnalité que l'on vérifiera l'équilibre entre la protection de la sphère privée des employés et les intérêts de l'employeur.

50 PFPDT, Guide, p. 13-18.
51 DUNAND, N 94 ad art. 328*b* CO.

Même si ce principe paraît parfois compliqué et théorique, il n'est souvent que l'expression du bon sens. Pour savoir si les mesures de surveillance sont proportionnées, l'employeur devrait se poser les questions suivantes :

- est-ce que j'ai vraiment besoin de toutes les données traitées ?
- est-ce que je peux atteindre le même résultat par un moyen moins intrusif ?
- est-ce que j'ai besoin de conserver les données aussi longtemps ?
- est-ce qu'il n'y a pas des personnes qui ont potentiellement accès aux données alors qu'elles n'en ont pas absolument besoin ?
- est-ce que les intérêts que je cherche à protéger ne pourraient pas l'être avec d'autres moyens ?
- est-ce qu'une surveillance anonyme ne suffirait pas à atteindre le but visé ?
- est-ce qu'il y a des buts inavoués autres que le but officiel de la surveillance ?
- est-ce que l'information donnée aux travailleurs est suffisamment claire et complète ?

Le principe de proportionnalité s'exprime aussi dans la gradation du choix des mesures de surveillance. L'employeur recourra principalement à des contrôles anonymisés et si besoin par sondage à des contrôles sur une base pseudonymisée (non nominale). Un contrôle nominatif ne devrait avoir lieu qu'en cas de soupçons fondés.

L'article 26 OLT 3 tolère une surveillance pour d'autres motifs que la surveillance du comportement des travailleurs. Au sens de la LPD, cela correspond aux intérêts privés prépondérants de l'employeur (art. 13 LPD). Une surveillance sans but précis ou sans raison est prohibée. La seule curiosité de l'employeur, tout comme l'éventualité qu'un quelconque résultat puisse à un moment ou à un autre être utile, ne constitue en aucun cas des motifs suffisants. Au sens du Code pénal, le consentement de la personne concernée, qui ne peut intervenir qu'avec une information suffisante, est un motif justificatif.

B. Cas d'application

1. La surveillance téléphonique

En l'absence de règlement ou d'informations particulières, il est difficile de savoir si l'usage du téléphone à titre privé est permis. Dans un tel cas, on considérera généralement que l'usage privé du téléphone est autorisé dans les limites du raisonnable.

L'employeur peut aussi, en se basant sur son droit d'édicter des directives et des instructions (art. 321*d* CO), interdire l'usage privé des appareils de l'entreprise et/ou d'un téléphone privé sur le lieu de travail. Cette interdiction ne pourrait néanmoins en aucun cas justifier une surveillance du contenu des appels privés effectués avec l'appareil de l'entreprise, ni une quelconque surveillance du téléphone privé. A noter que même si les

appels privés sont interdits, cela n'inclut pas la réception des communications privées sur son lieu de travail[52].

Si l'employeur a interdit l'usage privé, encore faut-il qu'il fasse respecter cette interdiction. En effet, l'employeur qui émet une directive interdisant les appels privés, mais qui dans les faits les tolère, ne peut pas prétendre ensuite dans le cadre d'une surveillance que le contenu des appels est exclusivement professionnel[53]. Cet élément est important et souvent méconnu : nombre d'employeurs croient en effet à tort qu'ils peuvent simultanément laisser les employés avoir des communications privées et se réfugier derrière une directive qui les interdit pour avoir les mains plus libres en cas de surveillance.

Quant à l'appareil privé utilisé dans le cadre professionnel par l'employé avec l'accord de l'employeur (BYOD[54]), la question est plus délicate et devrait être résolue au regard des circonstances du cas d'espèce et des conditions d'utilisation qui ont été prévues. Dans le cas où rien n'a été convenu, une surveillance paraît bien difficile à justifier. Elle ne pourra de toute façon porter que sur les contenus exclusivement professionnels.

L'employeur doit, dans tous les cas, laisser la possibilité au travailleur de mener une conversation privée, laquelle ne peut en aucun cas être sujette à surveillance par l'employeur. Ainsi, pour que la sphère privée du travailleur soit protégée, il faut pouvoir distinguer les appels privés des appels professionnels. Si les appels privés émis depuis les appareils de l'entreprise sont tolérés, il revient à l'employeur de prendre les mesures organisationnelles nécessaires pour que les numéros d'appels correspondant aux appels privés ne soient pas visibles (par exemple sur les factures). Si cela n'est techniquement pas réalisable, les employés doivent en être préalablement informés afin qu'ils puissent utiliser un autre appareil s'ils le souhaitent. L'employeur ne doit pas laisser penser aux travailleurs que les appels privés sont protégés et séparés, s'ils ne le sont pas[55].

L'utilisation d'un préfixe avant les appels privés permet de les traiter comme tels lorsque l'entreprise a par exemple un central téléphonique interne. Si cela n'est pas possible, ou si les bureaux sont partagés, il faut prévoir une cabine téléphonique ou un local à disposi-

52 PFPDT, Explications surveillance téléphonique, p. 1.

53 ALDER, p. 277.

54 « *Bring your own device* », soit « apportez votre propre appareil» est une pratique consistant pour l'employeur à autoriser (voire encourager) ses employés à utiliser leurs propres appareils à des fins professionnelles. Cela pose de nombreux problèmes juridiques et une politique de CYOD (« *Choose Your Own Device* » pour « choisi ton propre appareil ») est souvent préférable. Cette nouvelle tendance consiste à permettre aux collaborateurs de choisir parmi plusieurs appareils préapprouvés par l'employeur celui qu'ils veulent utiliser dans le cadre professionnel. Ces appareils restent néanmoins la propriété de l'employeur.

55 PFPDT, Explications surveillance téléphonique, p. 2-3.

tion des travailleurs dans lequel ils ne sont pas surveillés[56]. L'employeur n'est en revanche pas tenu de prendre en charge le coût des communications privées. La solution la plus simple, et la plus couramment utilisée actuellement, est de permettre aux employés d'utiliser leurs téléphones portables privés pour émettre et recevoir des appels privés dans une mesure raisonnable, au besoin dans une salle libre de l'entreprise s'ils partagent un espace de travail.

Si l'employeur soupçonne un abus ou un non-respect des directives, il devra procéder comme indiqué dans son règlement. Si l'employeur constate par exemple une augmentation globale des coûts facturés par l'opérateur téléphonique et qu'il a de forts soupçons d'abus, il devrait dans un premier temps examiner sur une base non nominale les numéros responsables des plus grands volumes de communication. Dans un deuxième temps, un examen des fichiers d'appels des quelques personnes concernées pourrait être effectué. En dernière mesure, un contrôle limité du contenu serait envisageable. Dans tous les cas, les personnes concernées doivent être informées préalablement et avoir la possibilité de s'y opposer[57]. La possibilité doit être donnée à l'employé de justifier l'augmentation éventuelle avant qu'une analyse détaillée ne soit effectuée. Si des explications suffisantes permettent de justifier la différence (par exemple en raison d'un séjour professionnel à l'étranger), il n'y aurait plus de but légitime à analyser les données secondaires.

Le contenu des conversations privées, qu'elles soient effectuées au moyen d'un appareil de l'entreprise ou au moyen du téléphone privé, ne peut jamais faire l'objet d'une surveillance par l'employeur, car une telle surveillance n'est pas nécessaire à l'exécution du contrat de travail et ne peut pas être justifiée. Si une surveillance de conversations identifiées comme privées devait néanmoins avoir lieu, par exemple en lien avec la commission d'infractions pénales, cette surveillance doit être opérée par les autorités d'instruction compétentes[58]. L'employeur pourrait tout au plus être tenu d'assister l'autorité pénale ou de tolérer l'exécution de la surveillance[59]. Il n'en prendra toutefois ni l'initiative, ni la responsabilité.

La surveillance d'appels professionnels est en revanche possible mais dans le strict respect des conditions posées par la loi. L'enregistrement des conversations à titre de preuve est assez courant dans certaines branches professionnelles et peut avoir lieu si tous les participants à la conversation en ont été informés. L'utilisation de ces enregistrements ne

---

56 PFPDT, Explications surveillance téléphonique, p. 2. Nous rejoignons l'avis de MEIER qui considère qu'actuellement l'employeur n'est plus obligé de mettre en place une cabine téléphonique ou un ordinateur avec accès à Internet vu l'omniprésence des téléphones portables (MEIER, p. 702-703). Un endroit pour les utiliser à l'abri de tiers nous semble néanmoins toujours justifié.

57 Voir aussi PFPDT, Banques.

58 Art. 269 ss CPP.

59 Art. 1 al. 4 LSCPT.

sera néanmoins possible que dans le but indiqué (à titre de preuve, de formation, etc.). Une fois le but indiqué atteint, l'enregistrement n'a plus de raison d'être conservé et doit être détruit[60]. L'enregistrement d'appels de détresse pour le compte de services d'assistance, de secours ou de sécurité n'est pas punissable, de même que l'enregistrement dans le cadre de relations d'affaires d'une conversation portant sur des commandes, des mandats, des réservations ou d'autres transactions commerciales de même nature (art. 179^{quinquies} CP).

2. La surveillance de l'Internet

Les règles sont similaires à celles applicables à la surveillance du téléphone. L'employeur doit indiquer s'il accepte ou non un usage privé de l'accès à Internet.

En l'absence de directive ou de règlement d'utilisation, une utilisation raisonnable d'Internet à des fins privées doit être jugée admissible, tant qu'elle ne concerne pas des sites dangereux, qu'elle ne porte pas atteinte à la réputation de l'entreprise et qu'elle n'empiète pas (ou seulement très marginalement) sur le temps de travail de l'employé, ni n'occasionne des coûts importants[61].

Si un usage privé est autorisé, ou à tout le moins toléré, les sessions privées ne devraient à un aucun moment faire l'objet d'une surveillance. Cela signifie qu'un moyen technique doit être donné au travailleur de signaler son activité comme privée et d'en soustraire le contenu à la surveillance de l'employeur.

Si l'employeur devait constater un abus dans l'usage privé, par exemple parce que l'un des employés consacrerait une part excessive de son temps de travail sur Internet à titre privé, une identification anonyme des sites visités et du temps consacré sera souvent de nature à résoudre la question. L'employeur n'a en effet pas besoin de connaître le contenu des sites visités pour pouvoir prendre des sanctions basées sur le droit du travail. Si le but est d'éviter la consultation de certains sites dont l'usage n'est pas requis professionnellement et auxquels l'employeur ne veut pas que les employés se connectent, il peut en bloquer l'usage[62]. L'employeur n'aura que rarement un intérêt justifiant une surveillance étendue de l'accès à Internet de l'employé. Pour l'activité qui n'est pas signalée comme privée, ou si toute activité privée est interdite, l'employeur devrait procéder principalement à des contrôles anonymisés et parfois, par sondage, à des contrôles sur une base non nominale (pseudonymisée) des fichiers de journalisation des ordinateurs de

60 PFPDT, Explications surveillance téléphonique, p. 4.

61 MEIER, p. 711.

62 Si certains utilisateurs ont des besoins plus étendus, il est toujours possible de leur donner plus d'accès (en mettant leur adresse IP sur une liste blanche par exemple).

l'entreprise. Un contrôle nominatif ne doit avoir lieu qu'en ultime recours et en cas de soupçons fondés.

A part dans de très rares hypothèses, en particulier dans le cas d'une obligation légale, l'enregistrement complet de toutes les sessions informatiques des utilisateurs, y compris l'accès à Internet, ne sera pas permis. Dans les cas exceptionnels où un intérêt suffisant et proportionné de l'employeur est admis, l'enregistrement ne se fera que dans un but de conservation à titre de preuves et l'accès aux données ne sera possible que dans des cas bien délimités (par exemple en cas de procédure ou requête judiciaire). Une surveillance générale et préventive est en tous les cas excessive, non justifiée et contraire au principe de proportionnalité.

3. La surveillance du courrier électronique

Les principes sont les mêmes que ceux concernant l'usage du téléphone. Pour des questions de sécurité, il est parfois préférable à l'employeur que ses employés n'utilisent qu'exclusivement leur adresse professionnelle. La séparation entre courriels privés et professionnels est en revanche plus aisée à réaliser[63]. Il suffit par exemple d'indiquer dans l'objet la mention « [privé] » et/ou de classer les messages envoyés et reçus dans des dossiers intitulés comme tels. Toute mesure de surveillance devrait alors exclure ces catégories. Dans le cas où la mesure de surveillance a lieu avant que l'utilisateur n'ait pu accéder à ses messages, il ne pourra pas les indiquer comme privés.

Il est difficile pour le travailleur d'empêcher des tiers de le contacter, y compris à titre privé, par le biais de son adresse électronique professionnelle. Dans une telle hypothèse, l'employeur devra prendre toutes les mesures possibles pour éviter autant que faire se peut l'accès à des courriels privés et renoncer à toute analyse dès qu'il constate que leur contenu n'est pas professionnel. Une surveillance de ce type est justifiée par exemple si les données doivent être conservées intégralement à titre de preuves, ou de manière automatique et anonyme par l'utilisation d'un logiciel de sécurité. Dans ces cas, l'atteinte à la sphère privée sera contenue : dans la première hypothèse, l'accès au contenu ne sera que très rarement effectué et obéira à des règles précises[64]. Et dans la deuxième hypothèse le processus sera automatique et anonyme.

---

63 L'interdiction totale du courrier électronique à des fins privées nécessite un énorme effort de contrôle, raison pour laquelle une telle interdiction reste la plupart du temps illusoire : PFPDT, 20e rapport, p. 73.

64 En particulier qui peut y accéder, à quelles conditions et dans quel but ; comment l'employé en sera informé et quelles seront ses possibilités de soustraire le contenu privé, etc.

A noter que même si l'usage privé est interdit, cela ne donne pas encore le droit à l'employeur de prendre connaissance du contenu d'un message privé non autorisé[65]. En cas d'absence prolongée du travailleur, se pose la question de l'accès par un tiers à sa messagerie. Si seul l'usage professionnel est autorisé, on peut se demander si l'intérêt de l'employeur à ce que la boîte électronique de l'employé ne reste pas inaccessible durant une période prolongée lui donne le droit d'y accéder. Cela présuppose toutefois que le travailleur en ait été informé préalablement et qu'il ne puisse lui-même pas y accéder (qu'il n'en ait pas la possibilité ou qu'il ait choisi de ne pas le faire par exemple pendant ses vacances). L'accès de l'employeur ne devrait pas porter sur des messages privés reçus. Si l'usage privé est autorisé, ou à tout le moins toléré, un accès par l'employeur ou un autre employé semble difficile à justifier. Dans tous les cas, on peut se demander si l'accès au message peut être considéré comme proportionné puisqu'il existe des moyens moins intrusifs, comme l'envoi automatique d'un message à tous les expéditeurs de messages non lus par exemple, sans avoir à consulter le contenu des courriels.

En effet, si un employeur doit faire face à une absence prolongée, il est recommandé d'ajouter simplement un message de réponse automatique pour tous les nouveaux messages, voire les messages déjà reçus depuis le début de l'absence du travailleur, indiquant que les messages reçus ne seront pas lus et qu'il est demandé à l'expéditeur de les réadresser à un autre employé. Cela peut être mis en place sans accéder au contenu de la boîte électronique et au contenu des messages et il est admis que le responsable informatique puisse activer automatiquement un tel message. Cette solution doit être privilégiée car c'est le seul moyen d'informer les correspondants et il n'est pas nécessaire d'accéder personnellement aux contenus des courriels[66].

A l'issue des rapports de travail, l'adresse doit être désactivée et les messages supprimés[67]. Si l'adresse n'est utilisée qu'à titre professionnel, l'employeur peut accéder au contenu. Il s'abstiendra néanmoins de prendre connaissance d'un éventuel message privé. Si l'usage privé était autorisé ou ne serait-ce que toléré, l'employeur n'a aucun droit d'accéder aux messages privés. Il doit alors donner la possibilité au travailleur de les récupérer sur un support privé, puis de les effacer des serveurs de l'entreprise[68]. Si l'employeur procède à une journalisation automatique (et systématique) de tous les messages entrant et sortant, il ne sera pas possible de retirer les messages privés. C'est alors au stade de l'exploitation éventuelle de ces données que des mesures devront être prises,

65 MEIER, p. 703.

66 PFPDT, 20e rapport, p. 73.

67 Sous réserve d'obligations légales de conservation, en particulier pour les entreprises soumises à l'obligation de tenir une comptabilité (art. 962 CO) : ALDER, p. 276-277.

68 DUNAND, N 103 ad art. 328*b* CO.

soit en donnant alors la possibilité à l'employé de procéder à un tri[69], soit par un processus automatisé qui retirera les messages ultérieurement marqués comme privé. Dans tous les cas l'employé devra aussi avoir été informé préalablement de la journalisation.

4. La surveillance de l'activité

Les moyens techniques actuels permettent très facilement de mettre en place des mesures particulièrement invasives sans que l'employé ne s'en aperçoive. On peut penser à une caméra vidéo, un logiciel espion qui retient chaque frappe du clavier, un outil d'analyse en temps réel d'analyse de l'utilisation et du comportement de la machine (et de son utilisateur), des captures d'écran en continu et en temps réel, un contrôle à distance des micros et caméra de l'ordinateur, etc. On peut aussi y ajouter l'utilisation pour un autre but que celui prévu de données disponibles (historique du navigateur Internet, historique des appels, données de facturation du téléphone, fichier journal des différents programmes, etc.).

Une telle surveillance doit répondre à des motifs stricts. La surveillance des travailleurs n'est pas admise pour surveiller le comportement des travailleurs à leur poste de travail, à moins qu'il y ait des impératifs liés à la prévention des accidents, la protection de la santé ou la sécurité des biens et des personnes, des motifs liés à l'organisation ou à la planification du travail, ou encore des objectifs de contrôle de la qualité des prestations ou du rendement ou de formation des employés. Dans ces cas, les employés devront être complètement informés et la mesure de surveillance devra être proportionnée.

La surveillance par curiosité de l'employeur est interdite. Une surveillance générale du comportement des travailleurs en dehors de leur travail, de leurs fréquentations, leurs usages des réseaux sociaux, leurs loisirs, etc. est évidemment interdite car elle ne correspondrait à aucun intérêt légitime de l'employeur.

C. Les conséquences d'une surveillance illégale

1. L'illégalité de la surveillance

Le travailleur qui fait face à une surveillance illégale peut réagir de plusieurs manières. Premièrement, sur la base des articles 15 LPD et 28 CC, il peut obtenir la prévention/cessation de l'atteinte, notamment l'interdiction du traitement, la rectification et la destruction des données, la constatation du caractère illicite de l'atteinte, et la communi-

[69] Cela pose la difficile question de retrouver les anciens employés, parfois plusieurs années après qu'ils ont quitté l'entreprise, et de leur capacité à trier des messages reçus longtemps auparavant.

cation à des tiers ou la publication de la décision le constatant[70]. Le travailleur peut également obtenir une réparation du dommage subi (art. 97 ss CO), voire dans certains cas intenter une action en remise de gain (art. 423 al. 1er CO)[71].

Deuxièmement, l'employé peut saisir les inspections cantonales du travail, également sur une base anonyme[72]. Ces offices et services cantonaux peuvent alors effectuer des visites sur place et rendre des décisions sous menace de la peine prévue à l'art. 292 CP, s'opposer à l'utilisation d'installations, voire, dans les cas extrêmement grave, fermer l'entreprise pour une période déterminée (art. 51 ss LTr). Dans la pratique, les autorités cantonales adresseront d'abord un avertissement à l'employeur. S'il n'est pas respecté, elles rendront alors une décision qui peut combiner les sanctions administratives et la menace de la peine de l'art. 292 CP.

Troisièmement, le travailleur peut déposer une plainte pénale pour violation des art. 179 ss du CP. Il n'obtiendra pas dans ce cas de modification directe de son environnement de travail, mais une condamnation pénale de l'employeur. La plainte peut viser tant la surveillance que dans certains cas l'utilisation de son résultat[73]. Une demande civile de dommages et intérêts pourrait être liée à la procédure pénale[74].

Quatrièmement, dans le cas où une méthode de traitement porte atteinte à la personnalité d'un nombre important de personnes, le Préposé fédéral à la protection des données pourrait recommander de modifier ou cesser le traitement. Si l'employeur ne se conforme pas à la recommandation du Préposé, ce dernier devrait alors saisir le Tribunal administratif fédéral pour obtenir son exécution (art. 29 ss LPD)[75].

2. Le résultat de la surveillance

L'illégalité de la mesure de surveillance ne rend pas systématiquement son exploitation impossible. Néanmoins, le Tribunal fédéral a déduit du droit à un procès équitable au sens des articles 29 al. 1 Constitution et 6 paragraphe 1 CEDH, l'interdiction de principe d'utiliser des preuves acquises illicitement. L'exclusion de tels moyens n'est toutefois

70 DUNAND, N 109-117 ad art. 328*b* CO.
71 MEIER, p. 578-582.
72 PFPDT, 20e rapport, p. 72.
73 Par exemple l'art. 179quater al. 2 CP qui sanctionne le fait de tirer profit d'un fait parvenu à sa connaissance au moyen de l'infraction de l'article 179quater al. 1 CP (soit d'observer sans le consentement de la personne intéressée avec un appareil de prise de vue ou d'enregistrer un fait qui relève du domaine secret de cette personne ou un fait ne pouvant être perçu sans autre par chacun et qui relève du domaine privé de celle-ci).
74 Art. 122 ss CPP.
75 MEIER, p. 613-623.

pas absolue et, cas échéant, le juge doit opérer une pesée des intérêts en présence. Ces règles sont applicables également aux procédures régies par la maxime d'office. L'utilisation de moyens de preuves acquis en violation de la sphère privée ne doit par ailleurs être admise qu'avec une grande réserve[76].

En procédure pénale, on distingue les preuves inexploitables car issues d'une méthode interdite (art. 140 CPP) telles que la contrainte, la menace, la tromperie, etc. ou les preuves mentionnées comme telles par le CPP, notamment les informations recueillies lors d'une surveillance non autorisée (art. 271 et 277 CPP). Des preuves relativement inexploitables (art. 141 al. 2 CPP), soit celles qui sont exploitables si elles sont indispensables à élucider une infraction grave et pourraient être recueillies légalement. L'autorité pénale, bien qu'elle soit généralement assez encline à admettre les preuves que lui remet le plaignant, devra néanmoins procéder à une pesée d'intérêts si la surveillance était illégale (y compris au sens du droit civil). La preuve qui aurait pu être obtenue légalement sera généralement admise.

En procédure civile, le Tribunal ne prend en considération les moyens de preuves obtenues de manière illicite que si l'intérêt à la manifestation de la vérité est prépondérant (art. 152 al. 2 CPC). Dans sa pesée d'intérêts, le juge tiendra compte de l'atteinte portée à la personnalité de l'employé, de l'intérêt de l'employeur à l'exécution de la surveillance, et des possibilités qu'aurait eu l'employeur de mettre en place un système moins invasif ou d'informer l'employé.

D. La réaction de l'employeur

Nous avons vu précédemment que des mesures de surveillance des travailleurs étaient légales et techniquement réalisables si certaines conditions sont remplies. Ces mesures de surveillance initiales auront lieu en l'absence de soupçon particulier de l'employeur et viseront généralement soit à récolter des informations en vue d'une éventuelle utilisation ultérieure (le plus souvent à titre de preuve en raison d'obligations légales), ou pour vérifier la bonne exécution du travail.

La position de l'employeur est particulièrement délicate lorsqu'il soupçonne la commission d'une infraction pénale ou d'autres violations de normes de droit civil, ou qu'un tiers lui a fait part de tels soupçons. En effet, si une infraction est dénoncée sur la base de faits non établis, une transmission à une autorité pénale expose l'employeur à des sanc-

76 ATF 139 II 7, JdT 2013 II 188 (rés.), SJ 2013 I 177 (rés.).

tions[77]. L'employeur doit ainsi procéder à une vérification préalable des faits qui lui sont dénoncés, la question concrète qui se pose alors à lui étant de déterminer le degré de certitude qu'il devra atteindre avant de transmettre, le cas échéant, la procédure à l'autorité compétente. L'employeur doit se limiter à élucider les faits en relation avec le travail de l'employé pouvant mettre en cause l'employeur et vérifier les éventuels motifs de licenciement immédiat[78].

L'art. 328 CO qui impose à l'employeur de protéger la personnalité du travailleur devra être interprété en ce sens que celui-ci devra être mis au bénéfice de garanties de procédures analogues à celles qui sont offertes par les procédures pénales. Ainsi doit-on lui accorder un droit d'être entendu, ce qui implique le droit de consulter le dossier, de s'expliquer, de produire des pièces, etc. Les moyens de surveillance déployés devront au surplus respecter l'art. 26 OLT 3 et la LPD[79].

Si le comportement du travailleur consiste uniquement dans la violation d'obligations contractuelles, c'est à l'employeur qu'il revient d'établir les faits et de prononcer les éventuelles sanctions. En revanche, si des infractions pénales sont commises, c'est le rôle de l'autorité policière et judiciaire[80]. S'il est nécessaire de réunir des preuves dans le cadre d'une poursuite pénale, il faut que ce soit sur ordre des autorités compétentes[81].

L'employeur privé n'a pas de devoir de dénonciation, contrairement aux employés de l'administration. Le personnel de la Confédération est notamment tenu d'annoncer aux autorités de poursuites pénales, à leurs supérieurs ou au Contrôle fédéral des finances tous les crimes et délits poursuivis d'office dont ils ont eu connaissance ou qui leur ont été signalés dans l'exercice de leurs fonctions[82]. L'employeur privé a en revanche le droit de signaler à l'autorité une infraction qui aurait été commise, même s'il n'en est pas la victime. Dans certains cas, il sera bien avisé de le faire pour éviter d'être accusé de complicité. La procédure pénale permettra aussi souvent de clarifier les faits et de justifier un éventuel licenciement pour justes motifs. L'employeur ne pourra souvent pas se permettre d'attendre l'issue de la procédure pénale, pour prendre une décision au regard du droit du travail. Souvent, il choisira de suspendre temporairement l'employé le temps de clarifier la situation. Un tel choix peut néanmoins avoir de lourdes conséquences pour le travailleur. L'employeur est donc contraint à un difficile exercice d'équilibrisme entre la préservation de ses intérêts, l'atteinte la plus légère possible à l'image et la personnalité

77 Par exemple pour atteinte à l'honneur (art. 173 ss CP), éventuellement dénonciation calomnieuse (art. 303 CP) ou induction de la justice en erreur (art. 304 CP).
78 BETTEX, p. 165.
79 BETTEX, p. 171.
80 SECO, p. 1.
81 PFPDT, Explications surveillance téléphonique, p. 3.
82 Art. 302 CPP et 22*a* LPers.

du travailleur et l'envie de préserver la réputation de l'entreprise, voire de contribuer à une saine administration de la justice.

L'employeur peut donc être en droit de mener des enquêtes et d'organiser des mesures de contrôle en vue de sauvegarder les moyens de preuves, d'empêcher la commission de l'infraction ou de préparer des sanctions ou des procédures judiciaires ultérieures. Les limites fixées par les règles générales sur la protection des données et les règles du droit du travail doivent être scrupuleusement respectées. L'employeur pourra néanmoins se fonder sur un intérêt privé prépondérant pour ne pas informer préalablement la personne mise en cause des mesures de surveillance qu'il entend prendre à son égard[83]. En principe, les entités de droit public ne peuvent pas se prévaloir d'intérêts prépondérants, mais doivent avoir prévu dans la loi les conditions auxquelles une telle surveillance peut être opérée[84].

Il n'y a pas de procédure ou de réponse toute faite pour déterminer la meilleure réaction de l'employeur. En revanche, si celui-ci s'est doté d'un règlement qui précise clairement ce qui peut être fait, par qui, dans quel cas et avec quelles conséquences, la plupart des problèmes seront résolus. L'employeur devra faire attention de développer une approche graduée dans les différentes analyses auxquelles il va procéder et d'informer dès que possible l'employé. Il pourra notamment enregistrer des données, qu'il n'exploitera qu'après avoir informé le travailleur. Dès qu'il a les informations suffisantes dont il a besoin pour décider des mesures à prendre au sens du droit du travail, l'employeur n'a plus de motifs pour continuer la surveillance. Il peut transmettre les informations aux autorités pénales s'il le souhaite.

IV. Conclusion

La surveillance des travailleurs n'est pas régie par une seule norme, mais par plusieurs lois dont les principes ont été complétés par la pratique des tribunaux, mais surtout par des directives et commentaires d'autorités administratives (PFPDT, SECO, etc.). Les grands principes présents dans ces différents textes sont néanmoins assez similaires et tendent à trouver un équilibre entre l'intérêt à la bonne exécution du travail et au respect des directives de l'employeur, et la protection de la sphère privée du travailleur. En se dotant d'un règlement clair et appliqué de manière cohérente, l'employeur limite grandement les risques de violation de la loi. Le travailleur informé correctement acceptera

83 DUNAND, N 94 ad art. 328*b* CO.

84 Au niveau fédéral, la Loi sur l'organisation du gouvernement et de l'administration judiciaire (LOGA) prévoit les différents types d'analyses autorisées aux articles 57*i* ss.

généralement mieux les intrusions (limitées) dans sa sphère privée et surtout pourra adopter un comportement afin de s'en protéger, ce qui ne signifie pas pour autant qu'il remplira moins bien ses obligations professionnelles. Une fois ce cadre posé, l'employeur devra avoir en tête le respect du principe de proportionnalité et régulièrement se demander si la surveillance est nécessaire et utile, ou s'il y aurait un moyen moins intrusif d'atteindre le même but. Cela ne permettra pas de résoudre tous les cas, mais il pourra se prévaloir d'une approche cohérente et relativement facile à mettre en place.

L'employé dispose d'un certain nombre de moyens tant civils que pénaux pour faire cesser une mesure de surveillance illégitime. Il pourra également s'opposer, dans une certaine mesure, à l'exploitation des résultats issus d'une telle surveillance. Quant à l'employeur, la situation la plus difficile pour lui sera toujours de décider quelles mesures d'investigation et quelles suites il va donner lorsqu'il a des soupçons fondés, y compris à la question de savoir si dans le doute, il préfère fermer les yeux, dénoncer pénalement à tort, ou se séparer du collaborateur immédiatement ou dans le respect du délai usuel. Ce choix dépendra en particulier de la gravité des faits reprochés et des risques pour l'employé et l'employeur.

V. Bibliographie

ALDER DANIEL, E-Mail-Daten am Arbeitspaltz im Fokus von Datenschutz-und Arbeitrecht, Revue de l'avocat, Berne 2013, p. 276-279.

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

BELSER/EPINEY/WALDMANN, Datenschutzrecht : Grundlagen und öffentliches Recht, Berne 2011.

BETTEX CHRISTIAN, Le cadre légal des enquêtes internes dans les banques et autres grandes entreprises en droit du travail, SJ 2013 II, p. 157-175.

BREGOU PIERRE, Le pouvoir disciplinaire de l'employeur, Paris 2012.

BRUNNER/BÜHLER/WAEBER/BRUCHEZ, Commentaire du contrat de travail, Lausanne 2011.

CHAPPUIS BENOÎT, Les moyens de preuve collectés de façon illicite ou produits de façon irrégulière, in : WERRO/PICHONNAZ (édit.), Le procès en responsabilité civile, Berne 2011, p. 107-147.

CORBOZ BERNARD, Les infractions en droit suisse, Vol. I et II, 3e éd., Berne 2010.

COSTA GIORDANO, Internet- und E-Mail-Überwachung am Arbeitsplatz, Jusletter 9 janvier 2012.

DETERMANN/SPRAGUE, Intrusive Monitoring : Employee Privacy Expectations are Reasonable in Europe, Destroyed in the United States, Berkeley Technology Law Journal 979 (2011).

DUNAND JEAN-PHILIPPE, in : DUNAND/MAHON (édit.), Commentaire du contrat de travail, Berne 2013.

GEISER THOMAS, Interne Untersuchungen des Arbeitgebers : Konsequenzen und Schranken, Allgemeine Juristische Praxis 08/2011, p. 1047-1056.

JEANDIN NICOLAS, in : PICHONNAZ/FOËX (édit.), Commentaire romand, Code civil I, Bâle 2010.

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

MEILI ANDREAS, in : HONSELL/VOGT/GEISER (édit.), Basler Kommentar, Zivilgesetztbuch I, Art. 1-456 ZGB, Bâle 2002.

MÉTILLE SYLVAIN, Les enseignements à tirer de la surveillance illicite de magistrats et fonctionnaires par un service informatique, Jusletter 3 septembre 2012.

MONNIER GILLES, Le piratage informatique en droit pénal, sic ! 2009, p. 141-153.

PRÉPOSÉ FÉDÉRAL À LA PROTECTION DES DONNÉES ET À LA TRANSPARENCE, Explications sur la surveillance téléphonique sur le lieu du travail, Berne 2006 (cité : PFPDT, Explications surveillance téléphonique).

PRÉPOSÉ FÉDÉRAL À LA PROTECTION DES DONNÉES ET À LA TRANSPARENCE, Mesures techniques et organisationnelles : guide, Berne 2011 (cité : PFPDT, Mesures).

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).

PRÉPOSÉ FÉDÉRAL À LA PROTECTION DES DONNÉES ET À LA TRANSPARENCE, 20e Rapport d'activité 2012/2013, Berne 2013 (cité : PFPDT, 20e rapport).

PRÉPOSÉ FÉDÉRAL À LA PROTECTION DES DONNÉES ET À LA TRANSPARENCE, Note à l'attention des banques sur la transmission de données personnelles aux autorités américaines, Berne 2013 (cité : PFPDT, Banques).

ROSENTHAL/JÖHRI, Handkommentar zum Datenschutzgesetz, Zurich 2008.

SECRÉTARIAT D'ETAT À L'ÉCONOMIE (SECO), Commentaire de l'Ordonnance 3 relative à la Loi sur le travail, Berne 2013.

STAEGER/MEIER, Surveillance vidéo sur le lieu de travail – quelques enseignements tirés de l'arrêt du TF 9C_785/2010 du 10 juin 2011, Jusletter 16 avril 2012.

STRATENWERTH/JENNY/BOMMER, Schweizerisches Strafrecht – Besonderer Teil I, 7. Auf., Berne 2010.

SUBILIA/DUC, Droit du travail – Eléments de droit suisse, Lausanne 2010.

TESTER MARISA, Video- und GPS-Überwachung von Arbeitnehmenden, Jusletter 24 septembre 2012.

WYLER RÉMY, Droit du travail, 2e éd., Berne 2008.

Deuxième partie

Questions choisies

CAROLE AUBERT / RÉGINE DELLEY

Utilisation des réseaux sociaux par les travailleurs et les employeurs

Sommaire

		Page
I.	Notion de « réseaux sociaux »	134
	A. Introduction	134
	B. Tentative de définition	135
	1. La distinction entre réseaux sociaux et médias sociaux	135
	2. Typologie des réseaux sociaux	137
	C. Enjeux juridiques actuels	138
II.	Utilisation des réseaux sociaux : risques et enjeux	139
	A. Enjeux des réseaux sociaux pour l'entreprise	139
	B. Principaux risques liés à l'utilisation des réseaux sociaux	141
	C. Importance de l'utilisation des réseaux sociaux dans le cadre de l'entreprise - enquêtes démoscopiques récentes	142
	1. Au niveau mondial	142
	2. Et en Suisse ?	143
III.	Réseaux sociaux et droit du travail	144
	A. Problématique du cadre juridique applicable	144
	B. Du côté de l'employeur	145
	1. Obligation de protéger la personnalité du travailleur	145
	a) Généralités	145
	b) Conséquences de la violation de cette obligation	146
	2. Recherche de candidats	146
	3. Surveillance des réseaux sociaux	148
	a) Généralités	148
	b) Monitoring des réseaux sociaux (surveillance « *extra-muros* »)	149
	c) Consultation du compte de réseau social d'un employé	150
	4. Droit de donner des directives et des instructions (art. 321*d* CO)	151
	a) Généralités	151
	b) Contenu	152
	c) Limites	153
	C. Du côté du travailleur	154
	1. Obligation de diligence et de fidélité	154
	a) En général	154
	b) Obligation de conserver le secret sur certains faits	155
	c) Sanctions en cas de violation de l'obligation de diligence et de fidélité	156

2. Violation de l'obligation de diligence et de fidélité commise à travers les réseaux sociaux 157
a) Exemples de jurisprudences françaises 157
b) Synthèse – importance de la qualification publique ou privée des propos publiés sur les réseaux sociaux 158

IV. Autres problématiques 160

V. Conseils pratiques 161

VI. Conclusion 162

VII. Bibliographie 162

I. Notion de « réseaux sociaux »

A. Introduction

La limite entre vie privée et vie professionnelle devient de plus en plus floue, en particulier en raison de la convergence des médias numériques et des supports de communication. Nous sommes accessibles et connectés en tout temps, quel que soit l'endroit où nous nous trouvons. Difficile ainsi d'ignorer que ce qui est publié sur Internet peut être lu, vu ou entendu par pratiquement n'importe qui et ce, pour une durée indéterminée. Cette évolution provoque inéluctablement des répercussions importantes sur notre vie quotidienne, y compris sur notre vie professionnelle.

Le cas récent de deux employés de la Banque cantonale zurichoise ayant critiqué leur hiérarchie sur Internet et s'étant vus suspendre de leurs fonctions[1] et celui d'un haut-fonctionnaire de la Maison Blanche limogé pour ses critiques contre l'administration[2] illustrent la problématique qui sera traitée dans la présente contribution. Peut-il y avoir une discussion privée sur Internet ? Où se trouve la limite entre la liberté d'opinion et l'obligation de fidélité due à l'employeur ? Dans quelle mesure l'employeur a-t-il le droit de surveiller l'activité de ses employés sur les réseaux sociaux et cas échéant utiliser les informations ainsi collectées ? Même si la jurisprudence en Suisse est encore rare en comparaison avec les pays voisins, la problématique existe bel et bien et le monde du travail y est confronté de manière quotidienne.

1 Voir MAIR.

2 http://www.usatoday.com/story/news/politics/2013/10/23/white-house-official-fired-tweets/3167871/ (consulté le 23 octobre 2013).

Faut-il nécessairement légiférer pour autant ? D'une manière générale, le droit suisse peut être qualifié de technologiquement neutre. Cela a notamment pour conséquence que la législation ne doit pas être adaptée à chaque nouvelle évolution technologique ; au vu de la vitesse de cette dernière, cet aspect est positif. A l'inverse, la loi étant générale et abstraite, elle nécessite d'être interprétée pour être appliquée aux nouveaux concepts, ce qui implique en particulier une grande confiance vis-à-vis du juge dans l'application du droit. Ce n'est pas autrement qu'en a conclu le Conseil fédéral dans son rapport publié le 9 octobre 2013[3]. Selon ce dernier, les réseaux sociaux posent de nouveaux défis dans le domaine du droit, mais il n'est pas utile de créer une loi spéciale pour y répondre. Les nouveaux canaux de communication s'accompagnent certes d'une vaste palette d'avantages et de risques, mais l'expérience montre que le droit suisse ne présente pas de grosses lacunes. Selon le Conseil fédéral, appliquées à bon escient, les dispositions générales contenues dans les lois en vigueur apportent une réponse adéquate à la plupart des problèmes que posent ou que pourraient poser les plateformes sociales aux particuliers et à la collectivité.

B. Tentative de définition

1. La distinction entre réseaux sociaux et médias sociaux

Un réseau social est un ensemble d'identités sociales, telles que des individus ou des organisations, reliées entre elles par des liens créés lors d'interactions sociales[4]. Avant l'émergence des réseaux sociaux sur Internet spécifiquement, les sciences sociales ont créé un ensemble de concepts, de modèles et de recherches empiriques : cette sociologie des réseaux sociaux consiste à prendre pour objets d'étude non pas les caractéristiques des individus, mais les relations entre eux et les régularités qu'elles présentent, pour les décrire, rendre compte de leur formation, de leurs transformations, et analyser leurs effets sur les comportements. Ce courant, en s'appuyant sur des approches empruntées à l'ethnologie et aux mathématiques, a su ainsi se constituer un domaine propre[5].

D'une manière générale, on peut définir un réseau social comme une communauté d'individus ou d'organisations en relation directe ou indirecte, rassemblée en fonction de centres d'intérêts communs, comme les goûts musicaux, les passions ou encore la vie professionnelle[6]. Des expériences récentes ont exploré la théorie du petit monde ou des

3 Voir CONSEIL FÉDÉRAL.

4 http://fr.wikipedia.org/wiki/R%C3%A9seau_social (consulté le 1er novembre 2013).

5 MERCKLÉ, p. 3-4.

6 http://www.journaldunet.com/encyclopedie/definition/1053/41/21/social_networking.shtml (consulté le 20 octobre 2013).

six degrés de séparation[7]. Ainsi, en novembre 2011, Facebook[8] a publié une analyse de son anatomie révélant l'existence en moyenne de cinq degrés de séparation entre ses membres (quatre, si l'on se réfère uniquement aux États-Unis[9]). Ces expériences confirment qu'un petit nombre d'intermédiaires est suffisant pour connecter n'importe quelle personne à une autre par Internet. La question a été discutée par la suite de savoir si c'est le réseau social lui-même qui finalement induit une réduction de la distance entre deux utilisateurs (nombre de nœuds)[10]. Le « friending » provoquerait en fait plutôt la construction de nouveaux liens non redondants (« bridging ») que le renforcement des liens existants et de la redondance intra-groupe (« bonding »)[11].

L'émergence des réseaux sociaux est liée aux révolutions technologiques ; c'est ce qui a donné naissance au Web 2.0. L'expression « médias sociaux » est cependant de plus en plus utilisée et tend à remplacer le terme de Web 2.0 et recouvre les différentes activités qui intègrent la technologie, l'interaction sociale et la création de contenu[12]. Les médias sociaux utilisent l'intelligence collective dans un esprit de collaboration en ligne. Par le biais de ces moyens de communication sociale, des individus ou des groupes d'individus qui collaborent créent ensemble du contenu web, organisent ce contenu, l'indexent, le modifient ou le commentent, le combinent avec des créations personnelles en utilisant de nombreuses techniques (flux RSS, blogs, wikis, partage de photos et de vidéos, réseaux sociaux, bookmarking collaboratif, etc.) [13].

L'émulation des réseaux sociaux fonctionne sur deux principes que l'on peut résumer ainsi : « les amis de mes amis sont mes amis » et « les personnes qui partagent les mêmes centres d'intérêts que moi sont mes amis ». L'utilisation des réseaux sociaux vise notamment à se faire des relations et se constituer un réseau, retrouver ses anciens amis, partager de l'information, nouer des liens et créer ainsi du contenu qui sera partagé.

---

7 MERCKLÉ, p. 13.

8 https://www.facebook.com/notes/facebook-data-team/anatomy-of-facebook/10150388519243859 (consulté le 20 octobre 2013).

9 BACKSTROM/BOLDI/ROSA/UGANDER/VIGNA.

10 BOLDI /VIGNA.

11 MERCKLÉ, p. 85.

12 Wikipedia, Réseau social, http://fr.wikipedia.org/wiki/R%C3%A9seau_social (consulté le 1er novembre 2013), citant KAPLAN et HAENLEIN, Users of the World, unite ! The challenges and opportunities of social media, Business Horizons, vol. 53, Issue 1, January-February 2010, N 59-68.

13 Wikipedia, Réseau social, http://fr.wikipedia.org/wiki/R%C3%A9seau_social (consulté le 1er novembre 2013).

2. Typologie des réseaux sociaux

Les caractéristiques communes des réseaux sociaux sont en général les suivantes :

- Nécessité préalable de créer un compte et un profil utilisateur et d'accepter les conditions générales du service offert, sans possibilité de les négocier[14] ; si le service est gratuit, la contre-partie est un droit d'utilisation concédé au réseau social sur les contenus et les données mises en ligne par l'utilisateur (« *user generated content* »)[15]
- Existence d'un outil de recherche parmi les utilisateurs (notamment pour étendre le réseau)
- Moyen de mise en communication et de contact entre utilisateurs
- Moyen de partage et de diffusion des données
- Moyen de structuration identitaire.

Il existe des réseaux généralistes (Facebook, Twitter, Pinterest) ou spécifiques, tels que professionnels (Linkedin, Xing, Viadeo), portant sur des centres d'intérêts tels que la musique (last.fm), le partage d'images (Instagram) ou de vidéos (YouTube), ou encore géographiques (par exemple Renren, Weixin ou Sina Weibo, les plus grands réseaux sociaux chinois[16]). La communauté peut également être restreinte au cadre de l'entreprise, grâce aux réseaux intra-entreprise ou les outils collaboratifs de gestion de projets.

A noter que la concurrence est importante et des concentrations sont observées (Facebook a racheté Instagram, Google est propriétaire de YouTube, etc.). La concurrence des opérateurs du marché se déporte maintenant sur la capacité à proposer des connecteurs permettant l'interopérabilité des réseaux entre eux (bouton « j'aime » de Facebook ou publication sur Twitter possible depuis n'importe quelle autre plateforme). Les médias sociaux se développent de manière à devenir omniprésents dans la vie des utilisateurs (par exemple Instagram n'est disponible que via l'utilisation mobile)[17]. L'évolution est tellement rapide qu'il serait vain de dresser des listes des réseaux existants, sous peine d'être obsolète à l'heure de mettre sous presse.

---

14 Voir notamment KELLER, p. 188 ss.

15 KELLER, p. 188.

16 Pour la Chine, voir notamment les infographies suivantes : http://www.resonancechina.com/2013/05/06/china-social-media-landscape/ et http://www.techinasia.com/2013-china-top-10-social-sites-infographic/ (consultés le 1er novembre 2013).

17 Voir ROBERT.

C. Enjeux juridiques actuels

Chaque réseau présente ainsi ses spécificités. L'évolution technologique est constante, notamment avec l'intégration de nouvelles fonctionnalités (géolocalisation, *tagging* et reconnaissance faciale, contenus temporaires, etc.), ce qui ne va pas sans poser des problèmes en terme de protection et de sécurité des données en particulier avec l'utilisation faite de la masse d'informations récoltées très souvent à l'insu des utilisateurs concernés. La complexification des réseaux, liée à une perte de contrôle sur les données publiées, rend ainsi aiguë la nécessité de légiférer en matière de « droit à l'oubli numérique » voire de droit à l'autodétermination sur ses données personnelles[18]. En outre, une certaine maturité commence à faire surface : les exigences des utilisateurs et des législateurs vont croissant, notamment en matière de protection des données[19].

Récemment l'émergence du « Big Data »[20] a donné naissance à de nouvelles formes de marketing[21], créant certaines inquiétudes quant à l'utilisation des données personnelles des utilisateurs et l'exploitation commerciale de profils de personnalités auxquels auront contribué « activement » les internautes.

Cependant, les réseaux sociaux paraissent de plus en plus incontournables, en particulier pour la diffusion d'informations en relation avec l'entreprise. C'est ainsi que la publication d'informations financières via les réseaux sociaux fait désormais l'objet de directives aux USA de la part des régulateurs boursiers[22] .

L'accès non-discriminatoire aux réseaux sociaux est une question importante face à la position dominante de certains acteurs. En effet, il ne faut pas perdre de vue que les réseaux sociaux sont des entreprises privées fixant elles-mêmes les conditions de participation et d'utilisation de leurs services. Dès lors, ne pas pouvoir disposer de la page de

---

18 FLÜCKIGER, p. 837 ss.

19 Voir notamment les interventions des législateurs en particulier des Etats aux USA afin de protéger les mineurs et les employés.

20 90% des données mondiales disponibles en ligne ont été créées les deux dernières années. Parmi ces informations, seules 20% sont structurées de manière à pouvoir être analysées à l'aide d'outils traditionnels. Ainsi, les 80% restants constituent une masse non structurée de contenus issus de sources telles que les réseaux sociaux, les microbloggings, les sites de partage de photos ou de vidéos. D'où le développement d'outils tels que la visualisation afin d'exploiter les potentiels commerciaux représentés par ces « big data ».

21 « Social media marketing ».

22 Réglementation publiée par Federal Financial Institutions Examination Council ; http://www.occ.gov/news-issuances/federal-register/78fr4848.pdf (consulté le 20 octobre 2013) et recommandations de la Securities and Exchange Commission (« SEC ») http://www.sec.gov/News/PressRelease/Detail/PressRelease/1365171513574#.UmP_C1NlkYs (consulté le 20 octobre 2013).

son entreprise sur les principaux réseaux sociaux ou à des conditions différentes de ses concurrents pourrait poser des problèmes en termes de concurrence et d'accès au marché.

Enfin, la plupart des principaux réseaux sociaux ont leur siège aux USA et soumettent leurs relations juridiques, pour la plupart, au droit californien[23], ce qui peut poser d'importants problèmes juridiques et pratiques, en particulier en termes de droit applicable et de mesures à prendre en cas d'urgence (voir *infra* IV).

II. Utilisation des réseaux sociaux : risques et enjeux

A. Enjeux des réseaux sociaux pour l'entreprise

L'immédiateté et la visibilité avec laquelle l'information est distribuée sur les réseaux sociaux peut avoir un impact considérable, en particulier dans le contexte de l'entreprise. Les effets vont bien au-delà de la problématique de la visibilité d'une information. Si l'information trouve sa source dans les médias classiques et qu'elle suscite un certain niveau d'intérêt, les réseaux sociaux s'en emparent et contribuent à diffuser cette information à un public encore plus large. Ce *buzz* créé sur les réseaux sociaux devient lui-même une information reprise dans les autres médias, créant ainsi une boucle d'amplification de l'information[24].

La question pour l'entreprise n'est ainsi pas de savoir si elle doit être présente ou non sur les réseaux sociaux, car de fait les consommateurs ou ses employés n'ont pas attendu l'entreprise pour parler d'elle et de ses produits[25].

Parmi les principaux défis auxquelles l'entreprise est désormais confrontée dans le cadre de l'utilisation des réseaux sociaux, on peut citer notamment :

- La protection de son identité numérique (par exemple la réservation de noms d'utilisateur, l'ouverture de comptes au nom de sa raison sociale ou de sa marque sur les principaux réseaux sociaux[26])
- L'amélioration de la visibilité de l'entreprise sur Internet, en particulier dans les moteurs de recherche (référencement)

---

23 Voir note 119.

24 PERRON/JOUK, p. 624.

25 « Your brand isn't what you say it is ; It's what they say it is », cité par MARTY NEUMEIER, The Brand Gap : How to Bridge the Distance Between Business Strategy and Design, Berkeley, 2005.

26 Voir dans le présent ouvrage la contribution de TISSOT NATHALIE et SALVADÉ VINCENT, p. 227 ss.

- La gestion de sa réputation en ligne ou de son « E-réputation » (par le bais d'outils de veille et d'alertes).

L'entreprise peut toutefois aller au-delà d'une simple attitude défensive et de préservation des acquis, notamment en :

- Améliorant sa réputation, par une analyse et une écoute en temps réel pour répondre aux critiques et améliorer ses produits ou services
- Utilisant les réseaux sociaux comme outils de marketing, afin d'entrer en contact direct avec des (futurs) consommateurs, mais aussi des employés, des fournisseurs, des sous-traitants, etc.
- Facilitant l'interaction entre les clients et la fidélisation d'une communauté autour de ses marques et ses produits
- Mobilisant cette communauté et en l'impliquant (« *empowering your people and customers* »), par exemple pour trouver le nom d'un nouveau produit ou de nouvelles idées (par le biais de concours notamment).

Ces nouveaux modes de communication ne s'improvisent donc pas et de plus en plus d'entreprises confient ceux-ci à une personne spécifique dans l'entreprise, à savoir le « *community manager* ». En outre, toute l'entreprise doit être mobilisée et en particulier l'adoption d'une charte sur les réseaux sociaux, spécifique ou intégrée à une charte générale de sécurité informatique / usage de l'Internet est fortement préconisée (voir *infra* III.B.4).

Il est ainsi très important de sensibiliser les employés de l'entreprise quant aux conséquences possibles de propos diffusés sur les réseaux sociaux, tant pour l'entreprise que pour les employés eux-mêmes. Dans son rapport d'octobre 2013 sur les médias sociaux, le Conseil fédéral conclut du reste celui-ci par le besoin d'améliorer l'éducation aux médias et spécialement aux médias sociaux parmi la population en général et non seulement au sein des groupes cibles tels que les enfants et les jeunes[27].

En outre, l'entreprise peut être tentée de mettre en place un monitoring des réseaux sociaux pour savoir ce qui se dit à son propos. Or, l'observation des réseaux sociaux ne saurait cependant être effectuée au mépris des principes régissant la protection des données : le suivi de certaines personnes physiques ou morales identifiées ou identifiables équivaut à un traitement de données au sens de la Loi sur la protection des données[28]. Si

27 Voir CONSEIL FÉDÉRAL, p. 80-81.

28 http://www.edoeb.admin.ch/datenschutz/00683/00690/00691/00692/index.html?lang=fr (consulté le 1er novembre 2013).

ces données sont récoltées aux fins de surveiller les employés, les règles en la matière[29] trouvent application.

B. Principaux risques liés à l'utilisation des réseaux sociaux

L'entreprise est désormais clairement exposée sur les réseaux sociaux et doit pouvoir dès lors maîtriser sa communication et son image, voire préparer un plan de réponse en fonction des atteintes auxquelles elle pourrait être confrontée.

Il convient rappeler que le facteur humain est en général le premier risque pour les systèmes d'information. La sensibilisation des utilisateurs aux problématiques liées à l'utilisation des réseaux sociaux paraît ainsi primordiale.

Parmi les principaux risques identifiés liés à l'utilisation des réseaux sociaux auxquels doit faire face l'entreprise figurent notamment :

- L'atteinte à la réputation (par exemple en cas de dénigrement, de publication d'informations erronées, de propos tenus au nom de l'entreprise dérogeant notamment à sa ligne de conduite)
- L'atteinte au secret des affaires (notamment la publication de faits confidentiels à l'entreprise)
- L'engagement de la responsabilité de l'entreprise (responsabilité civile, contractuelle ou pénale ; également pour le comportement de ses employés)
- La perte de productivité et les conséquences financières qui y sont liées (en raison par exemple du temps passé sur les réseaux sociaux par les employés ou de toutes autres atteintes sur les réseaux sociaux pour lesquelles l'entreprise devrait prendre des mesures)
- L'atteinte à la capacité de stockage ou à la bande passante de l'entreprise (en cas d'utilisation abusive de visionnage de vidéos par exemple)
- La mise en danger de la sécurité des données et des applications de l'entreprise (disponibilité, confidentialité, intégrité), par l'installation de logiciels étrangers pouvant véhiculer des virus.

Il ressort de cette liste non exhaustive que certains risques peuvent être minimisés par la politique interne de l'entreprise, notamment des mesures techniques (telles que des restrictions des droits d'administration sur le parc informatique, le blocage de l'accès à

[29] Voir dans le présent ouvrage la contribution de MÉTILLE SYLVAIN, p. 99 ss.

certains sites, la prévention et la formation des utilisateurs, etc.). Toutefois ces mesures ont aussi leurs limites légales et technologiques[30].

C. Importance de l'utilisation des réseaux sociaux dans le cadre de l'entreprise - enquêtes démoscopiques récentes

1. Au niveau mondial

Il ressort d'une enquête[31] réalisée en 2012 au niveau mondial auprès de multinationales de dix-neuf pays différents que plus des trois-quarts de celles-ci utilisent les médias sociaux à des fins professionnelles. Pour une majorité d'entre elles, cette utilisation est récente et a débuté au cours des deux années précédant l'enquête.

La moitié des entreprises autorisent l'accès à leurs employés à des sites de médias sociaux au travail pour une utilisation non professionnelle, mais environ un quart limitent cette autorisation à certains employés seulement. Elles sont moins d'un quart à interdire un usage non professionnel et à peine plus à bloquer complètement l'accès de leurs employés aux médias sociaux.

De manière générale, en 2012 les employeurs ont un comportement plus positif vis-à-vis des médias sociaux par rapport aux années précédentes, en particulier pour des utilisations non professionnelles. En 2012, ils étaient plus de 40% à considérer comme un avantage d'autoriser leurs employés à utiliser les médias sociaux tant pour des activités professionnelles que non-professionnelles ; à noter que ce taux a augmenté par rapport à 2011, où il ne s'élevait qu'à 30%. Entre 2011 et 2012, davantage d'employeurs ont en revanche surveillé l'utilisation par leurs employés des sites de médias sociaux ; le taux est ainsi passé de 27 à 36%. Ils sont également plus nombreux à avoir adopté une politique d'entreprise concernant l'utilisation des médias sociaux (55% en 2011 et 69% en 2012). La plupart ont introduit de nouvelles règles couvrant l'usage tant au travail qu'en dehors du travail.

Presque la moitié des employeurs ont dû faire face à des utilisations impropres des médias sociaux. Malgré ce taux élevé, seulement un tiers des employeurs se propose de former ses employés à l'usage approprié des médias sociaux. À peu près un tiers des entreprises ont déjà dû prendre des mesures disciplinaires contre leurs employés suite à de mauvaises utilisations des médias sociaux. Des clauses de résiliation avec une protec-

30 Voir dans le présent ouvrage la contribution de MÉTILLE SYLVAIN, p. 114 ss.

31 Social Media in the Workplace Around the World 2.0 de Proskauer's International Labor & Employment Law Group (http://www.proskauer.com/files/uploads/Documents/2012_ILG_Social_Network_Survey_Results_Social_Media_2.0.pdf) (consulté le 1er novembre 2013).

tion expresse en cas de mauvaise utilisation des médias sociaux après le départ des employés se retrouvent dans seulement 17% des contrats.

2. Et en Suisse ?

Une étude[32] menée sur la base d'un sondage en ligne réalisée en mars 2013 auprès de 881 entreprises, organisations sans but lucratif, organismes gouvernementaux et administrations suisses, renseigne sur le comportement des employeurs suisses[33] vis-à-vis des réseaux sociaux.

La proportion d'entreprises suisses présentes sur les réseaux sociaux, soit 67%, est un peu moins importante qu'au niveau mondial. Les grandes entreprises de plus de 250 employés y sont présentes à 89% (en baisse de 5% par rapport à 2012). Quant aux PME jusqu'à 10 employés, 59% d'entre elles recourent aux réseaux sociaux, ce taux ayant par contre augmenté par rapport à 2012 (56%). La majorité des entreprises ayant renoncé à utiliser les réseaux expliquent leur décision par le fait que cela représentait un investissement trop lourd.

Pour près de la moitié des entreprises, un budget et du personnel sont spécialement attribués à cette tâche ; en moyenne, c'est un poste à 64% qui est consacré à la gestion de la présence de l'entreprise sur les réseaux sociaux.

La majorité des entreprises indiquent utiliser les réseaux sociaux à des fins de communication globale afin de profiler leur marque et intègrent ceux-ci à leurs activités de marketing et de communication. Seules 13% des entreprises font usage des réseaux sociaux pour la vente directe de leurs produits et une minorité (10%) intègrent les données clients à leur « *Customer Relationship Management* ».

Quant aux plateformes les plus utilisées par les employeurs suisses, il s'agit de Facebook (84%), suivi de YouTube (59%). Le réseau professionnel allemand Xing arrive en 3^{e} position (55%) et Linkedin en 6^{e} position seulement.

En résumé, les entreprises suisses sont déjà largement actives sur les réseaux sociaux, en exploitant les nouvelles possibilités commerciales et techniques de marketing.

32 Bernet ZHAW Studie Social Media Schweiz 2013 bernet.ch/studien.

33 A noter que seulement 5% des réponses à cette étude proviennent de la Suisse romande ou italienne.

III. Réseaux sociaux et droit du travail

A. Problématique du cadre juridique applicable

Les principaux risques et enjeux pour l'entreprise identifiés plus haut se retrouvent dans le cadre plus restreint des rapports contractuels de travail entre l'employeur et l'employé.

Il convient ici de rappeler l'absence de législation spécifique en la matière, actuelle ou même de *lege ferenda*[34]. En outre, la jurisprudence suisse ne peut en l'état être qualifiée d'abondante, les tribunaux n'ayant jusqu'ici été que peu amenés à juger des cas traitant de cette thématique. Toutefois, les dispositions des textes législatifs suisses à formulation souvent générale, peuvent être interprétées et appliquées de manière à permettre des solutions équilibrées. Dans un domaine en constante évolution, une législation spécifique n'est pas souhaitable. C'est le constat auquel arrive le Conseil fédéral[35], qui note que le droit matériel suisse est suffisant ; même si beaucoup de problèmes ne peuvent pas être résolus seulement à l'aide d'instruments juridiques, il relève que l'information et la sensibilisation des utilisateurs jouent un rôle non négligeable[36]. En outre, le contexte dépasse les frontières nationales du fait que la plupart des plateformes utilisées activement en Suisse ont leur siège à l'étranger. Une réglementation nationale n'aurait dès lors qu'une portée bien limitée[37].

Il convient alors d'appliquer le droit positif et cas échéant de l'interpréter à la lumière des évolutions technologiques ; le juge s'efforcera de ramener l'état de fait à des situations déjà connues et qualifier celui-ci indépendamment de son support de diffusion. Les principes généraux du droit et le bon sens guideront en général les parties. En outre, les jurisprudences étrangères donnent des pistes de raisonnement intéressantes transposables en droit suisse (voir *infra* III.C.d).

En matière de droit du travail, il s'agit de procéder à une balance des intérêts entre les droits et obligations de chacune des parties. On peut ainsi se baser sur les principes et dispositions découlant des lois générales et en premier lieu sur les dispositions du contrat de travail.

Parmi les obligations du travailleur, on retiendra en particulier l'obligation de diligence et de fidélité de l'employé (art. 321*a* CO), l'obligation d'observer les directives

34 CONSEIL FÉDÉRAL, page 82.
35 CONSEIL FÉDÉRAL, notamment ch. 4.8, p. 60.
36 CONSEIL FÉDÉRAL, notamment ch. 7, p. 75.
37 CONSEIL FÉDÉRAL, notamment ch. 7.1.2, p. 75.

générales et les instructions particulières données par l'employeur (art. 321*c* CO), ainsi que les règles sur la responsabilité du travailleur (art. 321*e* CO).

Quant aux obligations de l'employeur, l'obligation de protéger la personnalité du travailleur en général (art. 328 CO) et plus spécifiquement le traitement de données personnelles (art. 328*b* CO) donnent le cadre légal applicable en la matière. L'obligation pour l'employeur de protéger la santé et l'intégrité personnelle de ses employés, découle également de la Loi sur le travail (art. 6 LTr) et son ordonnance en matière de surveillance des employés (art. 26 OLT 3).

En outre, il ressort des différentes contributions de cet ouvrage que bien d'autres dispositions légales à vocation plus générale peuvent s'appliquer, notamment en matière de protection de la personnalité (art. 28 ss CC et LPD), de protection du droit d'auteur (LDA), de lutte contre la concurrence déloyale (art. 3, 5, 6, 23 LCD[38]), voire des dispositions pénales, telles que les infractions contre l'honneur et le domaine privé (art. 173 ss CP) ou encore l'atteinte aux secrets d'affaires (art. 162 CP).

B. Du côté de l'employeur

1. Obligation de protéger la personnalité du travailleur

a) Généralités

Lorsque l'employeur entend utiliser des informations relatives à un employé provenant des réseaux sociaux, il devra respecter la personnalité de celui-ci en application de l'art. 328 CO et veiller à ne pas porter atteinte à sa sphère privée, sa liberté d'expression[39], son image, voire de manière plus large son honneur[40].

Par sphère privée, il faut entendre les événements que chacun choisit de partager avec un cercle plus ou moins étroit de personnes, qu'ils soient ou non en relation avec la vie professionnelle[41]. Les exigences à respecter en matière de protection de la personnalité sont déterminées par rapport à des critères objectifs et peuvent varier en fonction de la nature de la profession exercée[42].

38 SUBILLIA-BIGLER, p. 215 ss.
39 BRUNNER/BÜHLER/WAEBER/BRUCHEZ, p. 141.
40 CARRUZZO/SANDOZ/JACCARD/MONTICELLI, V A3, 1.7 ss.
41 BRUNNER/BÜHLER/WAEBER/BRUCHEZ, N 2, p. 141.
42 FAVRE/MUNOZ/TOBLER, N 1.1 ad art. 328 CO et les réf. citées.

L'obligation de l'employeur de protéger la personnalité de l'employé existe durant les relations contractuelles, après la fin du contrat[43], mais également, selon la jurisprudence, déjà avant sa conclusion, soit durant les pourparlers contractuels[44].

L'auteur d'une telle atteinte ne se limite pas à l'employeur lui-même, en tant que personne physique, il peut également s'agir de l'un des organes d'une personne morale (art. 55 al. 2 CC), voire un auxiliaire de l'employeur (art. 101 CO), comme par exemple un supérieur du travailleur ou un collègue[45].

b) Conséquences de la violation de cette obligation

Suite à la violation de son obligation de protéger la personnalité du travailleur, l'employeur aura l'obligation de réparer le dommage causé à ce dernier sous forme de dommages-intérêts, déterminés en application des règles générales en matière de responsabilité contractuelle (art. 97 ss CO) ou découlant d'un acte illicite (art. 41 ss CO).

La réparation du tort moral pourra également être requise par l'employé pour autant que la gravité de l'atteinte le justifie. Pour cela, elle devra être objectivement d'une certaine gravité et avoir été subjectivement ressentie par la victime comme une souffrance morale suffisamment forte pour qu'il apparaisse légitime dans ces circonstances qu'une réparation soit donnée[46].

L'employé pourra en outre requérir la cessation du trouble, en demandant par exemple la mise hors service d'une caméra de surveillance ou tout autre mode de surveillance considéré comme illicite[47].

Finalement, la résiliation avec effet immédiat du contrat de travail par le travailleur sera envisageable, si on peut considérer que l'atteinte à la personnalité est suffisamment grave pour constituer un juste motif.

2. Recherche de candidats

Comme le relève le Conseil fédéral[48], il est de notoriété publique que les recruteurs se servent des moteurs de recherche sur Internet afin de se renseigner sur de futurs employés potentiels. Selon une étude publiée par le géant du recrutement Randstad en

43 ATF 130 III 699 et les réf. citées.
44 FAVRE /MUNOZ/TOBLER, N 1.2 ad art. 328 CO et les réf. citées.
45 FAVRE /MUNOZ/TOBLER, N 1.7 ad art. 328 CO.
46 FAVRE /MUNOZ/TOBLER, N 1.39 et 1.41 ad art. 328 CO et les réf. citées.
47 FAVRE /MUNOZ/TOBLER, N 1.43 ad art. 328 CO.
48 CONSEIL FÉDÉRAL, notamment ch. 4.6.2.1, p. 57.

2012[49], plus de 50 % des responsables des ressources humaines recourent aux réseaux sociaux, régulièrement ou occasionnellement, au cours du processus de recrutement. Parmi eux, 25% vérifient les informations des curriculums vitae fournis par les candidats. L'on peut toutefois légitimement s'interroger si ces chiffres ne sont pas largement en-deçà de la réalité : le Préposé fédéral à la protection des données et à la transparence parlant même d'une proportion de deux-tiers[50].

Souvent les utilisateurs n'ont pas conscience que les informations qu'ils ont postées sur une plateforme de réseautage social sont susceptibles, selon les paramètres de confidentialité de leur profil, d'être trouvées par les moteurs de recherche et donc par un futur employeur. Toutefois, face à l'émergence d'une prise de conscience collective de la valeur des données personnelles, de plus en plus d'utilisateurs se sentent concernés par la protection de leur vie privée. En outre, les acteurs de l'Internet sont de plus en plus sous pression afin de rendre attentifs les utilisateurs aux réglages nécessaires pour protéger leur vie privée. La responsabilité du paramétrage du profil sur un réseau social relevant de la sphère privée, elle repose donc principalement sur l'utilisateur de ce réseau[51].

A l'inverse, les utilisateurs des réseaux sociaux « professionnels », tels que LinkedIn, Xing ou Viadeo, sont en principe conscients que leurs profils peuvent être utilisés par les recruteurs ; c'est d'ailleurs dans ce but précis qu'ils ont créé un profil personnel sur une telle plateforme. En général, les candidats rejoindraient précisément les réseaux sociaux professionnels avant tout dans l'espoir d'être contactés par un futur employeur[52]. De même, la référence à un compte de réseau social figurant sur le CV d'un candidat constitue un consentement présumé du candidat pour y accéder[53].

Il faut toutefois distinguer les informations accessibles au public des informations protégées par une configuration adéquate du compte. Les premières, qui peuvent être trouvées par une simple recherche sur Internet, ne peuvent être cachées à l'employeur. Toutefois, si l'employeur découvre à cette occasion des informations embarrassantes pour le candi-

---

49 Randstad international trends and workplace survey report 2012, http://www.randstad.com/press-room/randstad-workmonitor/randstad-workmonitormarch2011.pdf (consulté le 23 octobre 2013).

50 http://www.edoeb.admin.ch/datenschutz/00683/00690/00691/00693/index.html?lang=fr (consulté le 1er novembre 2013).

51 Newsletter 1/2012 du PRÉPOSÉ FÉDÉRAL À LA PROTECTION DES DONNÉES ET À LA TRANSPARENCE, http://www. edoeb.admin.ch/dokumentation/00460/00461/index.html?lang=fr (consulté le 1er novembre 2013). *Contra* : STUTZ/GEIGER-STEINER, p. 213.

52 STUTZ/GEIGER-STEINER, p. 213.

53 Newsletter 1/2012 du PRÉPOSÉ FÉDÉRAL À LA PROTECTION DES DONNÉES ET À LA TRANSPARENCE, http://www. edoeb.admin.ch/dokumentation/00460/00461/index.html?lang=fr (consulté le 1er novembre 2013) ; EGLI, N 86, p. 10.

dat, il devra, dans tous les cas, lui donner l'occasion de s'en expliquer[54] ; en effet, rien n'indique que celles-ci soient conformes à la vérité. En revanche, plus délicate est la question de l'accès par les employeurs, via des profils de tiers, à des informations que des candidats à un poste révèlent sur les réseaux sociaux. Une telle démarche va évidemment trop loin et le consentement des utilisateurs n'est plus présumé, à mesure que l'accès à ces données est limité à un cercle privé d'utilisateurs ; il s'agit d'une violation des principes de la transparence et de la proportionnalité. En effet, l'auteur des informations exprime explicitement par ses réglages de profil son souhait de rester dans une sphère privée et de préserver la confidentialité de ses données.

Face au phénomène, inimaginable en Europe, d'entreprises américaines exigeant des candidats qu'ils leurs remettent les codes d'accès afin de consulter les données qu'ils ont publiées sur des réseaux sociaux ou qu'ils se connectent pendant un entretien d'embauche, les législateurs des Etats américains ont commencé à légiférer en masse depuis début 2013 pour interdire une telle pratique (« *shoulder viewing* »[55]). Outre la commission d'une violation claire de la sphère privée, les recruteurs seraient ainsi également en mesure d'obtenir des réponses à des questions prohibées lors d'un entretien d'embauche, comme par exemple celles concernant l'orientation sexuelle, les opinions politiques ou la religion.

Il faut toutefois réserver le cas de certaines entreprises spécifiques sensibles, en particulier en matière de sécurité, qui doivent s'assurer du passé irréprochable des candidats[56].

3. Surveillance des réseaux sociaux

a) Généralités

L'employeur a un intérêt important à surveiller de manière générale l'utilisation faite par ses employés d'Internet. Il est légitimé de surveiller le travailleur du fait que ce dernier, de par son obligation de fidélité, a l'obligation de sauvegarder l'intégrité et la fiabilité des données de l'entreprise, notamment lorsqu'il en va de rapports avec des partenaires commerciaux (clients, fournisseurs, etc.), de respecter ses obligations légales et d'assurer

54 Newsletter 1/2012 du Préposé fédéral à la protection des données et à la transparence, http://www.edoeb.admin.ch/dokumentation/00460/00461/index.html?lang=fr (consulté le 1er novembre 2013).

55 Voir dans le présent ouvrage la contribution de COTTIER BERTIL, p. 18 s. Pour un aperçu de la pratique et des lois récemment adoptées, voir l'article du Wall Street journal du 22.04.2013, où l'on apprend que plus de 35 Etats américains ont légiféré depuis début 2013 http://online.wsj.com/news/articles/SB100014241278873 23551004578436713224083592 (consulté le 1er novembre 2013).

56 EGLI, p. 10.

une utilisation raisonnable et non dispendieuse des ressources de l'entreprise (tant en matériel qu'en personnel), notamment en vue de la rendre profitable. L'employeur doit cependant le faire en respectant les principes de protection des données, en particulier la proportionnalité[57]. Une telle surveillance « *intra-muros* » obéit ainsi à de strictes conditions nécessaires pour qu'elle soit admissible[58].

Le présent chapitre entend toutefois traiter l'aspect touchant la surveillance de l'activité des travailleurs sur les réseaux sociaux, par laquelle ceux-ci sont susceptibles de commettre des actes préjudiciables à l'entreprise, tels qu'une mise à mal de sa réputation ou la divulgation d'informations confidentielles. La surveillance de tels actes va clairement au-delà de la surveillance « *intra-muros* » effectuée notamment pour contrôler que l'employé ne fasse pas d'usage abusif des réseaux sociaux au détriment du temps de travail à consacrer à l'employeur.

b) Monitoring des réseaux sociaux (surveillance « *extra-muros* »)

Par le biais d'outils et de services en ligne permettant de balayer la toile, les employeurs peuvent obtenir des informations les concernant, diffusées notamment par leurs employés, sur les réseaux sociaux. Ce suivi systématique et permanent des informations publiées sur les médias sociaux (monitoring) pose problème dans le sens où il ne couvre pas seulement les contenus publiés sur ces réseaux, mais cette activité porte aussi sur des données dites sensibles[59] relatives à leurs auteurs[60].

Pour être admissible, ce traitement de données devra respecter la Loi sur la protection des données. En particulier, les résultats ne devront pas permettre d'obtenir des données permettant de faire un lien avec des données personnelles (identité, nom d'utilisateur de la personne qui a écrit un message, son âge, son sexe, sa profession, son employeur, etc.). Le monitoring devra se limiter à l'analyse d'opinions et de commentaires émis publiquement (notamment les données concernant un groupe non fermé d'utilisateurs ou un cercle d'amis)[61].

---

57 MEIER, N 2156, p. 697.

58 Voir dans le présent ouvrage la contribution de MÉTILLE SYLVAIN, p. 99 ss.

59 Art. 3 let. c LPD.

60 CONSEIL FÉDÉRAL, ch. 4.4.4.2, p. 44 ; Recommandations du PFPDT, Monitoring des médias sociaux et protection des données http://www.edoeb.admin.ch/datenschutz/00683/00690/00691/00692/index.html ?lang=fr#sprungmarke20_2 (consulté le 1er novembre 2013).

61 Cadre juridique pour les médias sociaux, CONSEIL FÉDÉRAL, ch. 4.4.4.2, p. 44, et Recommandations du PFPDT, Monitoring des médias sociaux et protection des données http://www.edoeb.admin.ch/datenschutz/00683/00690/00691/00692/index.html ?lang=fr#sprungmarke20_2 (consulté le 1er novembre 2013).

Du fait que la collecte de données par un monitoring conduit inévitablement à traiter des données personnelles, ce traitement devra donc se limiter au minimum nécessaire à l'exploitation des données et être effacé aussi vite que possible ou rendu anonyme[62]. La surveillance par ce biais de l'activité des employés sur les médias sociaux paraît ainsi compliquée sans violer la loi sur la protection des données.

L'employeur ne peut dès lors qu'être encouragé à agir en amont, en réglementant dans un document ad hoc les comportements des employés sur les réseaux sociaux en lien avec l'entreprise, qu'il juge admissibles ou non. D'autant plus, que si la manière d'utiliser Internet en général et les réseaux sociaux en particulier est réglementée, le contrôle est alors autorisé pour vérifier si l'utilisation est correcte. Dans de telles circonstances, le travailleur doit d'ailleurs s'attendre à ce que le respect d'un règlement soit contrôlé par l'employeur[63].

c) Consultation du compte de réseau social d'un employé

Pour mémoire, l'employeur n'a en principe pas le droit de consulter les supports de données appartenant à l'employé, tel que courriels, disques virtuels personnels, clés USB, CD-ROM, etc.[64]. Dans le sens où il s'agit de supports de données privés, les preuves réunies en violation de la personnalité d'un employé pourront en outre être jugées irrecevables par un tribunal.

A notre sens, cette interdiction ne vise pas uniquement les supports physiques mais également toutes les données ou documents enregistrés dans le *Cloud* ou un compte de type Dropbox ou Skydrive, protégé par un code d'accès. Le fait qu'un mot de passe et un nom d'utilisateur soient nécessaires pour en permettre l'accès leur donne la qualification de données privées. Ceci s'applique également aux informations contenues dans un compte de réseau social.

Ainsi, l'accès par l'employeur au compte sur un réseau social de l'employé « fermé » ou le fait d'en exiger le mot de passe ne saurait être autorisé sans que l'on considère qu'il s'agisse d'une violation de la personnalité de l'employé.

Toutefois, la consultation d'un support de données privé est envisageable lorsque deux conditions sont remplies : il doit exister un motif justificatif et un soupçon d'infraction reposant sur des indices concrets. Il y a motif justificatif si la personne concernée donne

---

62 Recommandations du PFPDT, Monitoring des médias sociaux et protection des données http://www.edoeb.admin.ch/datenschutz/00683/00690/00691/00692/index.html ?lang=fr#sprungmarke20_2.

63 CARRUZZO/SANDOZ/JACCARD/MONTICELLI, V F17.

64 PFPDT, Explications.

son accord ou si l'employeur ou l'entreprise a un intérêt prépondérant. L'intérêt qu'il y a à faire toute la lumière sur une infraction commise contre l'entreprise est considéré comme un intérêt prépondérant[65]. Toutefois, en l'absence de l'accord du travailleur, il paraît difficile d'obtenir les codes d'accès au compte de réseau social, sinon par le biais de mesures judiciaires (voir *infra* partie V).

4. Droit de donner des directives et des instructions (art. 321*d* CO)

a) Généralités

L'employeur a le droit de donner des directives générales sur l'exécution du travail et la conduite des travailleurs, ainsi que de leur donner des instructions particulières (art. 321*d* CO). Dès lors, l'employeur a également le droit de donner des directives en matière d'utilisation d'Internet et des réseaux sociaux, allant de la restriction (temporelle, matérielle, technique) jusqu'à l'interdiction totale[66].

Toutefois, du fait que la limite entre vie privée et vie professionnelle devient de plus en plus floue et que les employés consultent de plus en plus les réseaux sociaux de manière mobile, il devient difficile d'empêcher totalement leur usage sur le lieu de travail[67], à moins de conditions strictes de sécurité rendues nécessaires par le type d'entreprise ou la politique interne de l'entreprise en matière de BYOD (« bring your own device »)[68]. Malgré cela, une étude récente a montré que plus de 51% des employés sont prêts à contrevenir aux règles internes régissant l'utilisation des terminaux personnels et cette progression semble en forte hausse[69]. L'employeur peut en outre utiliser des mesures techniques, telles que des filtres pour bloquer l'accès à certains sites ou prévoir dans un règlement des listes négatives (accès interdit à des sites déterminés) ou positives (accès aux seuls sites expressément autorisés)[70].

---

65 PFPDT, Explications.

66 STUTZ/GEIGER-STEINER, p. 214 ; TF 4A_430/2008, consid. 4.1.

67 MEIER, N 2165, p. 700, et N 2171 et réf. citées, p. 702.

68 Le BYOD désigne la pratique de plus en plus courante (et parfois encouragée par l'employeur) consistant à apporter ses outils informatiques personnels (smartphones, tablettes, portables, etc.) et à les utiliser dans le cadre de ses activités professionnelles, entraînant par exemple une connexion au système d'information de l'employeur. Les problèmes juridiques posés par cette pratique (surveillance de l'employé, sécurité des données, sort des données, possibilité d'effacer les données à distances y compris les données privées de l'employé, etc.) dépassent toutefois le cadre de la présente contribution. En français : PAP, pour : « Prenez vos appareils personnels » ou encore AVEC, abréviation d'« Apportez Votre Equipement personnel de Communication ».

69 FORTINET.

70 MEIER, N 2199, p. 710.

En tout état de cause, prévoir des réglementations précises concernant l'utilisation professionnelle d'Internet, et plus particulièrement des réseaux sociaux, dans un règlement d'entreprise est fortement recommandé. A défaut, il sera très difficile de décider si l'utilisation faite d'Internet, respectivement des réseaux sociaux, est autorisée ou non, ou si le comportement de l'employé constitue une violation ses obligations contractuelles[71].

Le règlement adopté pourra être intégré à la charte générale de sécurité informatique, ou faire l'objet d'une charte séparée, comme l'usage de l'Internet, de la messagerie professionnelle ou des appareils BYOD.

Il est très important que les employés connaissent l'existence de ce document en le remettant non seulement lors de l'embauche, mais également à intervalles réguliers, notamment lors de mises à jour. Il s'agira également de le discuter et de l'expliquer, ceci dans un but de sensibilisation et de formation des utilisateurs des réseaux sociaux.

b) Contenu

Le contenu d'une telle charte peut être plus ou moins détaillé et il serait vain ici de tenter d'en dresser une check-list exhaustive[72]. Néanmoins, l'on peut mentionner les éléments suivants :

- Distinction selon l'usage privé ou professionnel, le premier pouvant être interdit de manière absolue[73]
- Conditions d'utilisation et d'accès (limitations horaires ou de durée, accès différencié selon la fonction occupée dans l'entreprise)
- Autorisation ou non de s'exprimer au nom de l'entreprise, qui peut être limitée à des personnes exerçant des fonctions particulières
- Interdiction de créer un compte sur un réseau social au nom de l'entreprise, de sa raison sociale ou de ses marques
- Obligation de signaler à l'employeur tout usage abusif par des tiers qui serait constaté ; interdiction d'y répondre directement ou personnellement sans y être formellement invité par l'employeur
- Règles sur le comportement social et le « savoir-vivre » sur les réseaux sociaux, même dans le cadre privé [74]

---

71 Voir *infra* p. 24.

72 Un site recense de nombreuses chartes d'utilisation des médias sociaux, surtout anglo-saxonnes : http://socialmediagovernance.com/policies.php (consulté le 1er novembre 2013).

73 L'employé n'ayant pas un droit à être connecté en permanence au monde extérieur, MEIER, N 2174, p. 703.

- Rappel de la nécessité de protéger les informations confidentielles et la propriété intellectuelle de l'entreprise
- Rappel de la directive générale en matière de sécurité informatique (mots de passe, etc.), si celle-ci existe
- Portée d'une possible surveillance ; échelonnement des sanctions en cas d'abus
- Formation, sensibilisation aux risques liés à l'utilisation des médias sociaux
- Sort des comptes après la fin des rapports de travail et des réseaux de contacts créés à titre professionnel (obligation de rendre compte et restituer au sens de l'art. 328*b* CO).

c) Limites

Ces directives doivent être en relation immédiate avec l'exécution du contrat de travail, ne pas sortir du cadre de ce qui est usuel et respecter le droit de la personnalité du travailleur[75]. Les modalités de l'exercice de ce pouvoir réglementaire varient selon les qualifications et les responsabilités du travailleur[76]. La possibilité d'édicter des règles de conduite en dehors de l'entreprise est soumise à des limites très sévères[77], notamment lorsque de telles règles sont nécessaires à la bonne exécution du contrat de travail[78], pour prévenir un conflit d'intérêts ou une activité du travailleur qui pourrait nuire ou faire concurrence à l'employeur[79].

A l'inverse, l'employeur peut prescrire à ses employés, par exemple dans le marketing ou le service clientèle, d'utiliser les réseaux sociaux dans le cadre de l'exécution de leur travail, en vue notamment d'élargir le cercle de clients ou assurer un support clientèle. Ces exigences sont admissibles pour autant que l'activité soit déployée pendant la durée de l'horaire de travail, qu'elle soit effectuée à l'aide de supports de communication fournis par l'employeur et que le profil de l'employé mentionne clairement son statut d'employé de l'entreprise[80].

---

74 Pour des exemples pratiques, voir notamment la charte de la Rega http://www.rega.ch/pdf/multimedia/Rega_Social_Media_Leitfaden_f.pdf ou de Kodak http://www.kodak.com/US/images/en/corp/aboutKodak/onlineToday/Social_Media_10_7aSP.pdf (consultés le 1er novembre 2013).

75 CARRUZZO/SANDOZ/JACCARD/MONTICELLI, II A5, N 4.

76 FAVRE /MUNOZ/TOBLER, N 1.1. ad art. 321*d* CO et les réf. citées.

77 FAVRE /MUNOZ/TOBLER, N 1.2. ad art. 321*d* CO et les réf. citées.

78 DUNAND, N 19 ad art. 321*d* CO.

79 WYLER, p. 136.

80 STUTZ/GEIGER-STEINER, p. 214 et réf. note 17.

C. Du côté du travailleur

1. Obligation de diligence et de fidélité

a) En général

L'employé actif sur les réseaux sociaux se doit de respecter son obligation de diligence et de fidélité vis-à-vis de son employeur conformément à l'art. 321*a* CO[81]. En matière d'utilisation des réseaux sociaux par les employés, est ici visé tout particulièrement l'aspect négatif de l'obligation de fidélité du travailleur, soit le fait pour celui-ci de s'abstenir de tout comportement susceptible de léser l'employeur dans ses intérêts légitimes et éviter, en particulier, de lui causer un dommage économique[82].

L'obligation de fidélité de l'employé commence dès le début de son activité et prend fin en même temps que les rapports de travail[83], soit à la fin du délai de congé et cela même si l'employé a été libéré de son obligation de travailler[84]. Cela signifie que si l'employé diffuse sur un réseau social, après la fin de son contrat de travail, des informations portant atteinte à son ancien employeur, celui-ci ne pourra invoquer qu'une responsabilité extracontractuelle (art. 41 ss CO).

En l'absence de directives ou d'un règlement d'entreprise, l'utilisation raisonnable d'Internet à des fins privées doit être jugée admissible[85]. Toutefois, lorsque l'employé utilise une partie non négligeable de son temps de travail à des consultations sur Internet de manière générale ou sur des réseaux sociaux en particulier, depuis sa place de travail et durant son temps de travail, il viole son obligation de fidélité[86]. L'employé doit tout son temps de travail à l'activité pour laquelle il a été engagé par l'employeur[87].

L'obligation de fidélité est liée au travail et ne s'étend en principe pas à la vie privée et sociale du travailleur[88]. Seuls les collaborateurs d'entreprises à vocation particulière (églises, partis politiques, syndicats, etc.) peuvent se voir imposer des critères de fidélité

81 Voir dans le présent ouvrage la contribution de DUNAND JEAN-PHILIPPE, pages 36 ss.
82 ATF 117 II 72, consid. 4a, JdT 1992 I 569.
83 WYLER, p. 108.
84 ATF 128 III 271, consid. 4a, JdT 2003 I 606.
85 MEIER, N 2202, p. 711.
86 Voir dans le présent ouvrage la contribution de DUNAND JEAN-PHILIPPE, p. 41 s.
87 WYLER, p. 108.
88 BRUNNER/BÜHLER/WAEBER/BRUCHEZ, N 4 ad art. 321*a* CO, p. 56.

plus sévères qu'une entreprise ordinaire, également hors de l'entreprise et dans leur vie privée[89].

Pour les employés d'entreprises ordinaires, l'obligation de fidélité ne saurait s'appliquer d'office aux comportements dans la vie privée. Toutefois, il est possible de déroger au contenu de l'obligation de fidélité, tel qu'il est défini par la loi, en précisant sa portée de manière extensive dans un contrat de travail ou un règlement d'entreprise. Les « *social media policy* » des entreprises fixent par exemple des règles sur la manière de s'exprimer, même au privé, au sujet de l'entreprise, notamment avec le recours à un « *disclaimer* »[90]. Une telle dérogation ne devra toutefois pas porter atteinte aux droits de la personnalité du travailleur et devra respecter le principe de proportionnalité applicable à la pesée des intérêts juridiquement protégés des deux parties[91]. L'obligation de fidélité trouve en effet sa limite dans le droit de l'employé au libre épanouissement de sa personnalité[92].

b) Obligation de conserver le secret sur certains faits

L'obligation de diligence et de fidélité comprend également l'obligation de conserver le secret sur certains faits[93]. Cette obligation de discrétion s'étend non seulement aux faits que l'employeur a expressément qualifiés de secrets, mais aussi à tous ceux dont il apparaît, selon les circonstances, que l'employeur veut interdire la divulgation[94]. La volonté de l'employeur qu'un fait déterminé soit tenu secret doit être reconnaissable par le travailleur[95].

L'employeur qui souhaite se protéger contre la divulgation d'informations ou de secrets liés à l'entreprise par l'employé sur les réseaux sociaux a intérêt à prévoir par écrit, par exemple dans un règlement d'entreprise ou une charte d'utilisation des réseaux sociaux, le type de faits qu'il qualifie de confidentiels. Il s'agira de préciser le contenu de cette obligation à nouveau lors de la fin du contrat. En effet, l'obligation de discrétion perdure au-delà de la fin du contrat de travail, à condition toutefois que l'employeur puisse justi-

89 FAVRE /MUNOZ/TOBLER, N 1.1 ad art. 321*a* CO.

90 Par exemple les directives de l'Office fédéral du personnel de la Confédération « Usage des médias sociaux », disponible sur la page (http://www.epa.admin.ch/dokumentation/publikationen/index.html ?lang=fr), « Social Media Principles » du groupe Roche, juin 2013 [http://www.roche.com/social_media_guidelines.pdf], celle de Apple (http://www.ifoapplestore.com/stores/apple_blogging-socialmedia_guidelines.pdf) (consultés le 1er novembre 2013).

91 BRUNNER/BÜHLER/WAEBER/BRUCHEZ, N 5 ad art. 321*a* CO, p. 57.

92 ATF 117 II 72, consid. 4a, JdT 1992 I 569.

93 Art. 321*a* al. 4 CO.

94 FAVRE /MUNOZ/TOBLER, N 4.1 ad art. 321*a* CO.

95 BRUNNER/BÜHLER/WAEBER/BRUCHEZ, N 10 ad art. 321*a* CO, p. 59.

fier d'un intérêt légitime à son maintien dans chaque cas particulier et qu'elle ne fasse pas obstacle au déroulement normal de la vie professionnelle du travailleur[96].

c) Sanctions en cas de violation de l'obligation de diligence et de fidélité

Le Tribunal fédéral ainsi que la doctrine considèrent que la sanction de l'obligation de diligence et de fidélité peut consister en une peine conventionnelle, si le contrat ou, éventuellement le règlement d'entreprise, le prévoit expressément. Des sanctions disciplinaires sont également envisageables. Elles peuvent prendre la forme du blâme, d'amende ou d'avertissement[97]. Elles doivent être proportionnées et, dans la mesure du possible, leur nature doit être préalablement déterminée. Leur application doit pouvoir être faite de manière impartiale et équitable et ne pas dépendre du bon vouloir de l'employeur[98].

Concernant l'amende, le règlement d'entreprise ne contient une réglementation adéquate à ce sujet que si les actes susceptibles d'entraîner une telle sanction sont suffisamment définis et pour autant que la procédure disciplinaire soit organisée selon les principes de l'Etat de droit. Le tribunal peut revoir non seulement la régularité de l'amende d'entreprise, mais également son montant[99].

L'établissement d'un règlement contenant des prescriptions précises est de manière générale recommandé. En effet, à défaut, des sanctions ne pourront être prises à l'encontre d'un employé que si un abus manifeste a été constaté[100]. De même, sans règlement, en cas de dommage causé à l'employeur, l'employé ne pourra être tenu responsable que des dommages qu'il a causés intentionnellement ou par négligence[101].

D'autres sanctions comme le blocage de l'accès à Internet ou le versement de dommages et intérêts et, dans les cas plus graves, la résiliation ordinaire ou immédiate du contrat de travail sont également possibles[102].

La publication d'un avis rectificatif, via les mêmes réseaux sociaux en cas de publication litigieuse afin de toucher un public similaire est par contre à éviter. En effet, en matière de réseaux sociaux, il convient de se montrer extrêmement circonspect, notamment quant

96 BRUNNER/BÜHLER/WAEBER/BRUCHEZ, N 10 ad art. 321*a* CO, p. 59.
97 CARRUZZO/SANDOZ/JACCARD/MONTICELLI, II A8 et les réf. citées.
98 FAVRE /MUNOZ/TOBLER, N. 1.17 ad art. 321*a* CO.
99 CARRUZZO/SANDOZ/JACCARD/MONTICELLI, II A8.
100 PFPDT, Guide 2007, ch. 10, p. 28.
101 PFPDT, Guide 2007, ch. 10, p. 28.
102 CARRUZZO/SANDOZ/JACCARD/MONTICELLI, VF 19 et 20.

aux retours désastreux en termes d'image qu'une communication maladroite peut provoquer[103].

2. Violation de l'obligation de diligence et de fidélité commise à travers les réseaux sociaux

a) Exemples de jurisprudences françaises

Vu l'absence de jurisprudence suisse traitant spécifiquement des conséquences d'une mauvaise utilisation des réseaux sociaux par les employés, il est intéressant, comme mentionné plus haut[104], de s'inspirer des jurisprudences étrangères.

Les tribunaux français ont eu l'occasion de rendre de nombreux arrêts depuis 2006 en lien avec des licenciements faisant suite à des propos dénigrants, diffamatoires ou injurieux, diffusés par les salariés sur les réseaux sociaux, et plus particulièrement sur Facebook.

Il ressort de ces arrêts des raisonnements intéressants concernant la manière de déterminer si les propos échangés sur les réseaux sociaux doivent être qualifiés de privés ou de publics.

La Cour d'appel de Besançon[105] définit Facebook de la manière suivante : [(…) le réseau Facebook a pour objectif affiché de créer entre ses différents membres un maillage relationnel destiné à s'accroître de façon exponentielle par application du principe « les contacts de mes contacts deviennent mes contacts » et ce, afin de leur permettre de partager toutes sortes d'informations ; que ces échanges s'effectuent librement via « le mur » de chacun des membres auquel tout un chacun peut accéder si son titulaire n'a pas apporté de restrictions ; qu'il s'en suit que ce réseau doit être nécessairement considéré, au regard de sa finalité et de son organisation, comme un espace public ; qu'il appartient en conséquence à celui qui souhaite conserver la confidentialité de ses propos tenus sur Facebook, soit d'adopter les fonctionnalités idoines offertes par ce site, soit de s'assurer préalablement auprès de son interlocuteur qu'il a limité l'accès à son « mur »].

Plusieurs arrêts relèvent que Facebook représente un espace public et privé et que la distinction se détermine en fonction des paramétrages du compte effectués par son utili-

103 Voir *infra* p. 30.
104 Partie III. A.
105 Arrêt de la Cour d'appel de Besançon du 15 novembre 2011.

sateur[106]. Par contre, d'un arrêt à l'autre, la manière de juger la conséquence de l'absence de preuve du paramétrage diffère.

En effet, dans un cas où il n'avait pas été établi que l'accès au profil du collègue sur le mur duquel l'employé avait écrit ses propos était bloqué, les propos ont été qualifiés de publics[107]. Dans un autre cas, aucune preuve ne permettait de dire que le compte Facebook de l'employé ou de ceux ayant participé aux échanges permettaient le partage à des personnes indéterminées, il a alors été jugé que les propos devaient être qualifiés de privés[108].

Par contre, lorsqu'il est prouvé ou admis que la page, sur laquelle les propos litigieux ont été écrits, est ouverte aux « amis des amis », permettant ainsi un accès ouvert, il a été jugé que ce mode d'accès à Facebook dépassait la sphère privée[109].

Dans le cas inverse, lorsque la preuve est apportée que le profil n'était ouvert qu'à très peu de personnes, lesquelles faisant partie d'une même communauté d'intérêts, la Cour de cassation française a jugé les propos comme étant privés[110].

b) Synthèse – importance de la qualification publique ou privée des propos publiés sur les réseaux sociaux

Sur la base de ces raisonnements, il est possible d'extrapoler la manière dont les tribunaux suisses pourraient appréhender des tels cas. Il convient en premier lieu de revenir sur l'importance de la distinction entre des propos diffusés sur des médias sociaux qualifiés de privés ou de publics.

Les propos privés sont couverts par le secret des correspondances et le droit au respect de la vie privée. En conséquence, l'employeur ne pourra valablement pas se baser sur de tels propos pour fonder une sanction ou justifier une résiliation avec effet immédiat sans violer son obligation de protéger la personnalité du travailleur.

En outre, une résiliation ordinaire fondée sur des propos qualifiés de privés pourrait être constitutive d'une résiliation abusive. En effet, de manière générale, il y a licenciement

106 Arrêt de la Cour d'appel de Reims du 9 juin 2010, Arrêt de la Cour d'appel de Rouen du 15 novembre 2011.

107 Arrêt de la Cour d'appel de Reims du 9 juin 2010.

108 Arrêt de la Cour d'appel de Rouen du 15 novembre 2011.

109 Arrêt du Conseil de prud'hommes de Boulogne Billancourt du 19 novembre 2010.

110 Arrêt de la Cour de cassation du 10 avril 2013 : dans ce cas, l'accès à l'information mise en ligne était limité à des membres choisis en nombre particulièrement restreint ; il s'agissait de 9 contacts sur MSN et 14 sur Facebook.

abusif lorsque l'employeur exploite les conséquences de sa propre violation du contrat ou de la loi pour justifier la fin des rapports de travail[111].

En tout état de cause, une telle preuve obtenue de manière illicite ne pourrait pas être prise en considération par un tribunal[112].

Au contraire, si les propos sont qualifiés de publics, l'employeur pourra valablement s'en prévaloir pour justifier une sanction ou une résiliation du contrat de travail et la preuve sera considérée comme valablement obtenue. En outre, la qualification de propos publics servira à démontrer la gravité de l'atteinte. En effet, le fait de diffuser des propos sur des réseaux accessibles à un grand nombre ou un nombre indéterminé de personnes, sera constitutif d'une faute d'autant plus grave.

Les juridictions suisses pourraient qualifier les propos échangés sur des réseaux sociaux de différentes manières :

1. Les réseaux sociaux pourraient être considérés comme un espace public sans qu'il soit nécessaire d'apporter une quelconque preuve du paramétrage du compte sur lequel les propos ont été tenus. Reprenant la définition de la Cour d'appel de Besançon[113], tout profil de réseau social serait présumé ouvert, à charge de l'auteur des propos d'apporter la preuve que son profil est limité. Le fardeau de la preuve appartiendrait ainsi à l'employé.
2. Les tribunaux pourraient au contraire retenir que la preuve de la qualification des propos doit être apportée par les parties. Ainsi, en cas de licenciement abusif, c'est l'employé qui invoquerait l'art. 336 CO qui devrait apporter la preuve que ses propos sont des propos privés. Par contre, en cas de licenciement avec effet immédiat, c'est à l'employeur qu'il reviendrait de prouver que les propos de l'employé revêtent un caractère public.
3. La preuve du caractère privé des propos est plus facile pour l'employé étant donné qu'il peut prouver les paramètres de son propre profil. Par contre, s'il s'agit de prouver les paramètres du profil d'une autre personne sur le mur duquel les propos ont été écrits, cela devient plus compliqué. Il en va de même pour l'employeur qui doit prouver le caractère public des propos de l'employé. La preuve est libre à mesure qu'elle demeure rapportée dans les limites fixées par les codes de procédure et permet de prouver des faits pertinents. Parmi les modes de preuves disponibles, l'employeur peut démontrer par des captures d'écran les propos figurant sur le mur de l'employé et le fait que malgré que ce dernier ne fasse pas partie de ses amis, il a

111 BRUNNER/BÜHLER/WAEBER/BRUCHEZ, N 3 ad art. 336 CO, p. 251.
112 Art. 152 al. 2 CPC, ATF 139 II 7, JdT 2013 II 188 (rés.), SJ 2013 I 177 (rés.).
113 Arrêt de la Cour d'appel de Besançon du 15 novembre 2011.

été en mesure de voir ces propos. Un témoin pourra également confirmer qu'il a eu accès aux propos sans être ami avec son auteur, ce que pourra également attester un constat notarié[114]. La preuve ainsi rapportée sera toutefois soumise à la libre appréciation du juge.

4. Le degré de la preuve du paramétrage du compte devra ensuite être déterminé. Le fait de prouver que le profil est restreint aux seuls amis de l'employé suffira-t-il à qualifier les propos de privés, tout en sachant que la plupart des profils comptent plusieurs centaines d'amis ? Faudra-t-il encore prouver que ces amis font partie d'une même communauté d'intérêt ou qu'ils sont en nombre très restreint. Enfin, jusqu'à quelle limite peut-on soutenir que les personnes susceptibles de lire les propos litigieux sont en nombre suffisamment restreint pour que ceux-ci puisse toujours être qualifiés de privés ?

Du fait que le paramétrage d'un compte de réseau social peut être modifié en quelques clics de souris, il faut pouvoir démontrer que le paramétrage était tel qu'il a permis, à un moment ou à un autre, de rendre les propos accessibles à un nombre indéterminé de personne ou à une communauté suffisamment large pour ne plus être qualifiés de privés (voir *infra* V).

IV. Autres problématiques

Il est certain qu'un employé a le droit de refuser de son supérieur ou de son employeur une demande d'ajout dans sa liste d'amis / contacts (ou vice-versa) mais cela peut évidemment le mettre dans l'embarras. Il s'agit à notre sens d'une question de bon sens : les parties devraient s'abstenir de solliciter l'établissement de tels liens hors des réseaux sociaux professionnels (tels que Xing ou LinkedIn). Cela permettra ainsi d'éviter que les parties soient mises face à des déclarations d'ordre privé gênantes et que notamment l'employeur utilise ces informations contre l'employé. En outre, un contact sur un réseau professionnel pourra être maintenu plus facilement après la fin des rapports de travail.

Comment prévenir une éventuelle violation d'une obligation de non-concurrence après la fin des rapports de travail ? S'il s'agit d'un compte créé dans l'exécution du travail, les accès du compte doivent être restitués à la fin des rapports de travail et cela évitera l'exploitation du réseau de contacts ainsi créé. Par contre, s'il s'agit d'un compte privé, les parties doivent avoir préalablement convenu que l'employé effacera de son compte les contacts réalisés dans le cadre de son activité professionnelle. En effet, on ne peut exiger que l'employé conserve un statut avec une situation qui ne reflète pas la réalité ou

114 AUBERT/RAMSEIER/RISSE.

qu'il lui soit fait défense d'effectuer une annonce générale de son changement de statut, qui ne vise pas directement les anciens collègues ou les clients de son ancien employeur.

V. Conseils pratiques

D'une manière générale, si l'une des parties au contrat de travail entend réagir à une publication sur un réseau social, plusieurs problèmes pratiques peuvent surgir.

Dans le cas d'une partie qui entend faire disparaître d'un réseau social un contenu constituant une atteinte à sa personnalité (art. 28 ss CC), l'éditeur ou l'hébergeur devra retirer le contenu litigieux à mesure qu'est considérée comme responsable toute personne dont la collaboration cause, permet ou favorise cette atteinte, sans qu'il soit nécessaire qu'elle ait commis une faute[115]. Toutefois, la difficulté d'une telle action provient du fait que la plupart des réseaux sociaux sont situés en Californie et soumis au droit de cet Etat[116].

Si les propos constituent une violation sur le plan civil, voire même une infraction pénale, il peut être parfois plus rapide de contacter le réseau social lui-même à l'aide des formulaires *ad hoc* prévus par celui-ci[117]. Même si le réseau social s'est réservé dans ses conditions générales de déterminer souverainement une éventuelle violation des conditions générales par l'utilisateur, celles-ci sont formulées de manière suffisamment large pour y motiver une demande d'effacement de données publiées pour violation des conditions générales d'utilisation.

En outre, les réseaux sociaux acceptent de manière informelle des requêtes directes des autorités de poursuites pénales, voire même des injonctions (mesures provisionnelles ou requêtes de preuve à futur) émanant de tribunaux civils sis à l'étranger [118].

Enfin et non des moindres, il faut garder en tête l'audience mondiale des propos tenus sur les réseaux sociaux. Ainsi, une réponse inadéquate ou disproportionnée à un contenu jugé offensant ou illicite peut avoir des effets démultipliés encore plus dommageables

115 TF 5A_792/2011 du 14 janvier 2013.

116 Voir par exemple pour Facebook (https://www.facebook.com/legal/terms) ou Twitter (https://twitter.com/tos) (consultés le 1er novembre 2013).

117 https://www.facebook.com/help/contact/274459462613911, https://support.twitter.com/groups/56-policies-violations#topic_238 (consultés le 1er novembre 2013).

118 Pour Facebook, voir https://www.facebook.com/safety/groups/law/guidelines/ et https://www.facebook.com/about/privacy/other (consultés le 1er novembre 2013) ; pour les utilisateurs hors Canada et USA, la filiale irlandaise est compétente, de sorte que la Convention de Lugano s'applique ! Pour la question de l'accès par les autorités, en particulier de poursuite pénale, directement à des données hébergées à l'étranger ou dans le cloud, voir l'article de WALDEN.

pour l'entreprise que si celle-ci n'avait tout simplement rien fait (« effet Streisand »[119] ou effet « Kitkat »[120]) et que l'atteinte initiale elle-même.

VI. Conclusion

On retiendra de la présente contribution que les entreprises auraient tort de se priver des nombreux avantages que représentent les réseaux sociaux. Toutefois, ils veilleront à se prémunir contre différents risques.

Une réglementation spécifique est en effet indispensable à plusieurs titres. En premier lieu pour déterminer si les employés sont autorisés à utiliser les réseaux sociaux en lien avec leur activité professionnelle, et dans l'affirmative, de quelle manière. Elle sera également nécessaire pour contrôler son respect et définir les sanctions en cas d'utilisation incorrecte.

Toutefois, la réglementation ne fait pas tout. Rien ne vaut une sensibilisation efficace des employés quant à la portée des propos publiés sans restriction sur les réseaux sociaux et les risques qu'ils peuvent occasionner. Dans une société où la limite entre vie professionnelle et vie privée devient de plus en plus floue, l'employeur se doit de protéger la vie privée de ses employés mais également les protéger d'eux-mêmes.

VII. Bibliographie

AUBERT/RAMSEIER/RISSE, La preuve numérique : notion et appréciation juridique, Revue de l'avocat 2007, n° 11/12, p. 487-491.

BACKSTROM/BOLDI/ROSA/UGANDER/VIGNA, Four Degrees of Separation, Università degli Studi di Milano, 2012, disponible en archive ouverte (http://arxiv.org/pdf/1111. 4570v3.pdf).

BRUNNER/BÜHLER/WAEBER/BRUCHEZ, Commentaire du contrat de travail, 3e éd., Lausanne 2004.

BOLDI/VIGNA, Four Degrees of Separation, Really, Università degli Studi di Milano, 2012, disponible en archive ouverte (http://arxiv.org/pdf/1205.5509.pdf).

119 http://en.wikipedia.org/wiki/Streisand_effect (consulté le 1er novembre 2013), nommé ainsi suite à la tentative de censure de la chanteuse Barbra Streisand sur la publication d'une image de la côte de Malibu sur laquelle figurait sa maison dans le cadre d'une étude sur l'érosion côtière en Californie ; suite à son intervention, le monde entier savait désormais où elle était domiciliée…

120 Tentative de censure par Nestlé d'une vidéo publiée sur YouTube par Greenpeace en relation avec l'utilisation de l'huile de palme détruisant les habitats des grands singes : http://www.vanksen.fr/blog/nestle-et-la-gestion-du-scandale-kit-kat/ (consulté le 1er novembre 2013).

CARRUZZO/SANDOZ/JACCARD/MONTICELLI, Le contrat de travail, Des pourparlers aux conséquences de la résiliation, Service d'assistance juridique et conseils de la Fédération des Entreprises Romandes, Genève 2003.

CONFÉDÉRATION SUISSE, Office fédéral du personnel de la Confédération OFPER, Usage des médias sociaux, Berne 2011, http://www.epa.admin.ch/dokumentation/publikationen/index.html?lang=fr.

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

DUNAND JEAN-PHILIPPE, in : DUNAND/MAHON (édit.), Commentaire du contrat de travail, Berne 2013.

EGLI URS, Soziale Netzwerke und Arbeitsverhhältnis, Jusletter, 17 janvier 2011.

FAVRE/MUNOZ/TOBLER, Le contrat de travail code annoté, 2e éd., Lausanne 2010.

FLUCKIGER ALEXANDRE, L'autodétermination en matière de données personnelles : un droit (plus si) fondamental à l'ère digitale ou un nouveau droit de propriété ?, PJA 2013, p. 837.

KELLER CLAUDIA, AGB von Social-Media-Plattformen, Medialex 2012, p. 188 ss.

MAIR STEPHANE, Schweigen oder fliegen, Handelszeitung, Zürich 3 octobre 2013.

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

MERCKLÉ PIERRE, La sociologie des réseaux sociaux, Paris 2011.

PERRON/JOUK, Risque réputationnel – les réseaux sociaux changent-ils la donne ?, Revue de l'expert comptable suisse 9/12, p. 624 ss.

PRÉPOSÉ FÉDÉRAL À LA PROTECTION DES DONNÉES ET À LA TRANSPARENCE, Explications relatives au droit d'un employeur de consulter les supports de données privés d'un employé qu'il soupçonne d'avoir commis une infraction (cité : PFPDT, Explications).

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'intention des administrations publiques et de l'industrie privée, décembre 2007 (cité : PFPDT, Guide 2007).

ROBERT VINCENT, Enjeux juridiques des médias sociaux, in : Développements récents dans l'environnement numérique, CEDIDAC, Lausanne 14 mai 2013.

STUTZ/GEIGER-STEINER, Arbeitsrechtliche Fragen Rund um Social Media, Revue de l'avocat 2013, p. 212 ss.

SUBILLIA-BIGLER NATHALIE, Plainte pénale pour concurrence déloyale ou clause de prohibition de concurrence, in : WYLER (édit.), Panorama II en droit du travail, Berne 2012.

WALDEN IAN, Accessing Data in the Cloud: The long Arm of the Law Enforcement Agent, in : Privacy and Security for Cloud Computing, sous la direction de Siani Pearson et George Yee, London 2012.

WYLER RÉMY, Droit du travail, 2e éd., Berne 2008.

SÉBASTIEN FANTI

Bref aperçu des aspects légaux du BYOD (Bring Your Own Device)

Sommaire

		Page
I.	Introduction, notions fondamentales	166
	A. Définition du BYOD	166
	B. Contexte général et sécuritaire	168
II.	Règles applicables en matière de droit du travail	170
	A. Nécessité et forme du consentement de l'employeur	170
	B. Consentement de l'employé (art. 327 al. 2 CO) et droit de révocation	171
	C. Horaires de travail	172
	1. Protection de la personnalité du travailleur (art. 328 CO) et obligation de déconnexion	172
	2. Vacances (article 329*a* CO et 329*d* al. 2 CO)	175
	3. Travail du jour et travail du soir (art. 10 LTr) ; interdiction de travailler la nuit (art. 16 LTr) ; dérogation à l'interdiction de travailler la nuit (art. 17 LTr)	176
	D. Frais professionnels (art. 327 al. 2 CO, 327*a* CO)	177
	E. Responsabilité en cas de dommage ou de perte (art. 321*e* CO)	178
III.	Règles applicables en matière de protection des données	179
	A. Atteintes à la personnalité de tiers	179
	1. Violation du principe de sécurité (art. 7 al. 1 LPD, art. 8 et 9 OLPD)	180
	2. Violation du principe de la bonne foi : perte de données (Data Breach) et devoir d'information (art. 4 al. 2 LPD)	183
	3. Communication transfrontière de données et exemple du *Cloud* (art. 3 let. f, 6 et 10*a* LPD)	185
	4. Difficultés engendrées par l'exercice d'un droit d'accès (art. 8 LPD)	188
	C. Atteinte illicite à la personnalité de l'employé (328*b* CO)	189
	1. Teneur et portée de l'article 328*b* du CO	189
	2. Sanctions de la violation de l'article 328*b* du CO	193
IV.	Règles applicables en matière de droit pénal	194
	A. Détérioration de données (art. 144bis CP)	194
	B. Violation de secrets privés (art. 179 CP)	196
V.	Règles applicables en matière de propriété intellectuelle	198
	A. Exception d'usage privé (art. 19 LDA)	198
	B. Droit sur des inventions et des designs (art. 17 LDA et art. 332 CO)	199
VI.	Charte BYOD (BYOD Policy)	200

VII. Conclusions 200
VIII. Bibliographie 201

I. Introduction, notions fondamentales

A. Définition du BYOD[1]

Littéralement, le terme BYOD se traduit par « apportez vos propres terminaux ». Il s'agit d'une pratique qui consiste à utiliser ses équipements personnels (téléphone, ordinateur portable, tablette électronique) dans un contexte professionnel[2]. Dans le cas typique, il s'agit du système d'information de l'entreprise d'un côté et, de l'autre, d'un dispositif privé comme un smartphone ou une tablette numérique[3]. La première fonctionnalité utilisée dans ce cadre est la synchronisation des courriels et de l'agenda. Il peut en résulter un mélange des données privées et professionnelles. Régulièrement, des outils permettant la lecture et/ou la modification de documents professionnels sont évoqués lorsqu'il s'agit de définir la notion de BYOD. Il existe, en fonction du type d'activité et des besoins de l'entreprise, une multitude d'outils qui peuvent entrer dans le cadre de cette définition. Citons, à titre exemplatif, les logiciels de prise de notes permettant de collecter de l'information et de l'organiser[4], les logiciels de gestion de tâches, les logiciels de dictée numérique, ceux de traduction, ou encore ceux de *Cloud computing*, etc.

La définition du BYOD est rarement l'œuvre de juristes, quand bien même elle est fondamentale pour en appréhender les enjeux et les risques. Elle se doit d'être technologiquement neutre et évolutive, sous peine d'apparaître rapidement surannée. À titre exemplatif, il n'existe aucune prospection relativement aux nouveaux outils susceptibles pourtant, à brève échéance, de générer des problèmes juridiques notables et singuliers, non évoqués à ce jour. Les Google Glass[5] vont très certainement impacter

1 Il est également régulièrement fait référence au BYOM, soit Bring Your Own Mobile, les deux termes étant presque équivalents. En français le terme utilisé pour désigner cette pratique est PAP, soit prenez vos appareils personnels.

2 http://fr.wikipedia.org/wiki/BYOD (consulté le 18 décembre 2013).

3 MÖSSNER, § 1.2, p. 3.

4 Comme Evernote.

5 http://fr.wikipedia.org/wiki/Google_Glass (consulté le 18 décembre 2013) : le projet Google Glass, ou Project Glass (projet lunette) est un programme de recherche et développement lancé par Google sur la création d'une paire de lunettes avec une réalité augmentée. Cette paire de lunettes est pour

durablement nombre d'activités professionnelles[6], nonobstant le fait de savoir s'il est opportun de qualifier le résultat de ce programme de recherche « de révolution »[7]. Des centaines de « little brothers[8] » vont-ils déferler dans l'entreprise ?

Comme le suggérait un rédacteur du New York Times en 1998 déjà[9] : « Peut-être avons-nous été si obsédés par l'idée d'éviter le Big Brother totalitaire d'Orwell que nous n'avons pas remarqué l'arrivée de millions de commères indiscrètes »[10]. Le BYOD engendre ainsi par essence une intrusion réciproque dans les univers personnels et professionnels qui peut se définir ainsi : l'utilisation dûment autorisée[11] et réglementée octroyée à certains utilisateurs du système d'information de l'entreprise liés à celle-ci par un contrat de travail[12] de recourir à leurs matériels personnels à des fins professionnelles[13]. Il en résulte évidemment des problèmes légaux en termes de protection des données, de droit du travail, de droit pénal et de droit de propriété intellectuelle. Nous

l'heure équipée d'une caméra intégrée, d'un micro, d'un pavé tactile sur l'une des branches, de mini-écrans et d'un accès à Internet par Wi-Fi ou Bluetooth.

6 Pour un aperçu des problématiques en matière de protection des données s'agissant de l'utilisation des Google Glass, cf. la prise de position du Groupe 29 dans une lettre adressée à M. Larry Page, CEO de Google Inc., lettre paraphée par le Préposé à la protection des données et à la transparence : http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2013/20130618_letter_to_google_glass_en.pdf et pour un avis d'utilisateur : http://www.bilan.ch/node/1010417 (consultés le 18 décembre 2013).

7 Selon THAD STARNER, Professeur au Georgia Institute of Technology : « *Google Glass will be as revolutionary as the automobile* », http://www.technologyreview.com/qa/515681/wearable-computing-pioneer-says-google-glass-offers-killer-existence/ (consulté le 18 décembre 2013).

8 En référence au *Big Brother* du roman 1984 de Georges Orwell (expression qui concerne désormais les pratiques portant atteinte aux libertés fondamentales et à la vie privée), les *little brothers* sont la démonstration du passage d'une société de surveillance à une société de sous-surveillance caractérisée par l'apparition d'un nombre infini de surveillants (par opposition au surveillant centralisé) au bénéfice de technologies répandues qui leur permettent de collecter des données ou d'accéder à des données partagées spontanément par tout un chacun.

9 LEWIS.

10 Traduction de WHITAKER, p. 192.

11 Selon certains auteurs, le consentement à l'utilisation du BYOD peut être tacite, lorsque l'employeur qui sait que ses collaborateurs utilisent leur matériel privé l'accepte sans réserves.

12 On ne saurait en effet parler de BYOD lorsque des tiers (livreurs, consultants, etc.) utilisent leur matériel en interaction avec l'infrastructure de l'entreprise.

13 Pour une autre définition, BERANEK ZANON, N 1 ; lorsque le matériel est propriété de l'employeur, on ne parle pas de BYOD ; il s'agit donc de l'élément de différenciation fondamental de la définition proposée.

traiterons donc des questions topiques dans ces domaines, la présente contribution ne prétendant évidemment pas être exhaustive[14].

B. Contexte général et sécuritaire

Le BYOD est une tendance inéluctable, pour différents motifs. Les travailleurs sont à l'évidence ravis de pouvoir bénéficier de l'utilisation d'appareils, qu'ils maîtrisent et leur productivité s'en trouverait notablement accrue, notamment s'agissant de l'investissement en heures supplémentaires[15]. La flexibilité est également un avantage indéniable, régulièrement mis en exergue : les salariés peuvent exercer une activité dématérialisée, en consultant par exemple leur agenda lors de leurs déplacements et il peuvent être joints de manière facilitée, même en dehors des heures de travail[16]. Le taux d'adoption des applications métier de l'entreprise va également croître, pour autant évidemment que celles-ci soient mobiles ce qui est l'un des défis de la direction informatique. Qui connaît les impacts d'un taux d'adoption rapide en termes financiers, soit les sommes engagées pour déployer de telles solutions appréciera le BYOD comme une opportunité.

De nouvelles pratiques vont très certainement émerger : *Bring your own Application, BYO Cloud, BYO Date, etc...*[17]. Une moralisation de l'activité professionnelle est également évoquée[18], en relation avec l'identification plus forte à l'image et aux intérêts de l'entreprise avec laquelle l'interconnexion est permanente. Finalement, pour un employeur n'ayant pas les moyens d'avoir du matériel aussi performant que ses salariés, cela peut représenter un choix stratégique et concurrentiel essentiel.

---

14 Les problèmes seront parfois surprenants : sur le plan fiscal quel est le statut de l'appareil ? En cas de décès de l'employé, quel sera le statut des données professionnelles ?

15 L'employé serait prêt à s'investir en moyenne 240 heures supplémentaires par an, cf. BERANEK ZANON, N 19.

16 Ce qui génère évidemment l'interrogation relative à la prise en considération de ces périodes comme du temps de travail.

17 Voir ANDY.

18 Information Commissioner's Office (ICO), Guidance : Bring Your Own Device, n° 6 et 7, http://www.ico.org.uk/~/media/documents/library/Data_Protection/Practical_application/ico_bring_your_own_device_byod_guidance.pdf ; ce document a été édité suite à un incident survenu en décembre 2012 au Royal Veterinary College, lequel a généré un engagement (undertaking) disponible ici : http://www.ico.org.uk/news/latest_news/2013/~/media/documents/library/Data_Protection/Notices/Royal-Veterinary-College-Undertaking.pdf (consultés le 18 décembre 2013).

En Suisse, le BYOD serait d'ores et déjà une réalité dans neuf entreprises sur dix, selon une étude d'Avanade[19]. En comparaison internationale[20], il s'agit de la démonstration d'une entrée en force dans le monde de l'entreprise, spécifiquement des tablettes.

Il existe évidemment des risques corrélatifs, liés entre autres à la fuite d'informations, à l'exposition des données personnelles, etc.[21]. De plus, la gestion du parc informatique peut s'avérer complexe et onéreuse pour une entreprise en fonction de sa taille et de ses compétences. Sans vouloir et devoir entrer dans des détails trop techniques, il convient de mettre en exergue le fait qu'un audit doit précéder l'implémentation. Cet audit portera, en substance, sur :

- l'identification du type de données traitées et de leur caractère sensible ;
- leur qualification (privée/professionnelle) ;
- la nature des données personnelles pouvant être traitées sur un appareil personnel[22] ;
- les *devices* (respectivement leur propriété ou leur détention au sein de l'entreprise) ;
- les groupes d'utilisateurs potentiels de ces appareils en fonction de leurs besoins et de leur rôle au sein de l'entreprise ;
- les services, respectivement les applications concernées par l'introduction du BYOD et celles qui devraient l'être pour accroître la productivité de l'entreprise ;
- l'impact de l'introduction du BYOD sur les services partagés avec des organisations tierces également du point de vue de l'éventuelle contravention à des accords existants ou à des droits de propriété intellectuelle ;
- l'accroissement hypothétique de l'utilisation des médias sociaux du fait d'un accès facilité, instantané et perpétuel ;
- l'induction éventuelle de failles de sécurité dans les environnements considérés comme « safe » de l'entreprise ;
- …[23]

Cet audit permettra une identification des problèmes juridiques et la mise en place d'une véritable stratégie BYOD. Les options diffèrent à l'aune de la taille de l'entreprise, de

19 Voir LELIÈVRE.

20 L'enquête a été réalisée en septembre 2012 auprès de 599 cadres et décideurs Technologie et Information dans 19 pays. Dans le monde, plus d'une entreprise sur six (61%), a déclaré que la majorité de ses employés utilisaient maintenant des appareils personnels au travail.

21 MORIN, p. 5.

22 Pour éviter des difficultés ultérieures, notamment en cas d'acte illicite, par exemple suite à un téléchargement en violation des droits d'auteur ou de fichiers pornographiques.

23 Pour de plus amples informations, cf. BERANEK ZANON, p. 2 ss (Prozess zu BYOD).

son secteur d'activité, des processus réglementaires à respecter, de sorte qu'il n'est pas objectivement possible de proposer une matrice.

À ce stade liminaire, la nécessité de préparer soigneusement l'introduction du BYOD est une évidence. Le large spectre des problématiques juridiques qui seront exposées ci-après achèvera de convaincre les plus réticents ou les plus impatients qu'il ne suffit pas d'opérer une connexion entre l'entreprise et ses salariés pour profiter en toute quiétude des avantages déjà exposés.

Le BYOD est sommes toutes un contrat de confiance entre employeur et employé où la transparence et la bonne foi doivent guider le processus complexe d'analyse, de formalisation et d'adoption. Pour ce faire, l'identification des risques juridiques est cruciale.

II. Règles applicables en matière de droit du travail

A. Nécessité et forme du consentement de l'employeur

La première question à résoudre a trait au fait de savoir si l'employeur doit ou non consentir à l'utilisation d'appareils privés par ses salariés dans le cadre professionnel. Selon l'article 327 alinéa 2 du CO, si, d'entente avec l'employeur, le travailleur fournit lui-même des instruments de travail ou des matériaux, il est indemnisé convenablement, sauf accord ou usage contraire. Cela signifie, sans doute possible, que l'accord de l'employeur doit être recueilli, à tout le moins tacitement. Ainsi, l'employeur qui s'abstient de se manifester alors qu'il sait que ses employés utilisent leurs appareils privés pourrait se voir objecter l'existence d'un tel consentement[24]. Relevons toutefois que l'employé qui utilise ses outils privés en l'absence de consentement explicite de l'employeur commet une violation de son devoir de loyauté[25], susceptible d'engager sa responsabilité. Il lui incombe dans une telle configuration d'opérer lui-même la séparation entre les données privées et professionnelles et de sécuriser son appareil.

24 REUTTER/KLAUS, p. 160 s.
25 BERANEK ZANON, N 17 à 29.

B. Consentement de l'employé (art. 327 al. 2 CO) et droit de révocation

L'employé peut-il s'opposer à l'introduction du BYOD ? En clair, s'agit-il d'une option ou d'une obligation ? C'est la deuxième hypothèse qui suscite des interrogations à ce stade de l'analyse. Si l'employeur veut imposer le BYOD, il devra procéder à une modification du contrat de travail. L'article 327 al. 2 du CO prévoit en effet que, si d'entente avec l'employeur, le travailleur fournit lui-même des instruments de travail ou des matériaux, il est indemnisé convenablement, sauf accord ou usage contraire. Si le contrat n'est pas modifié, cela signifie simplement que les salariés pourraient émettre des prétentions quant à une indemnisation. Le consentement est également nécessaire pour l'implémentation de dispositifs permettant de sécuriser les données professionnelles sur l'appareil privé[26], de même que pour la surveillance qui pourrait être opérée et l'éventuelle géolocalisation[27]. En sus, l'effacement à distance des données contenues dans la mémoire de l'appareil mobile, propriété de l'employé, ne peut à l'évidence intervenir qu'avec son accord formel, préalable et éclairé[28]. Certains auteurs considèrent qu'imposer le BYOD à l'ensemble des employés d'une entreprise est illusoire et ne constitue pas une décision sérieusement défendable[29]. Le choix d'obliger ou de proposer devra donc avant toute autre considération se calquer sur la nécessité de devoir disposer de tels outils. Il est par exemple difficilement concevable que le personnel de nettoyage puisse y trouver un quelconque bénéfice[30].

L'employé peut, quant à lui, décider en tout temps de ne plus accepter la pratique du BYOD. Pour éviter des difficultés pratiques et organisationnelles, il conviendrait de prévoir un délai de rétractation[31]. Cela n'est toutefois pas légalement possible à l'aune du fait que le consentement à un traitement de données peut, en principe, être révoqué en tout temps[32]. Il existe des limites à la révocabilité que le Tribunal fédéral évoque dans

---

26 ARNING/MOOS/BECKER, p. 592.

27 La plupart des solutions BYOD du marché prévoient la possibilité de géolocaliser les salariés en temps réel ce qui ne manque pas de générer un problème, le Tribunal fédéral ayant jugé que si une surveillance indirecte et intermittente est proportionnée, il n'en va pas de même d'une surveillance continue (ATF 130 II 425, consid. 4).

28 En cas de perte ou de vol notamment.

29 BERANEK ZANON, N 18.

30 Sauf à ce que la généralisation du recours aux robots n'intervienne à brève échéance.

31 Un délai de 30 jours paraîtrait à cet égard raisonnable. Certaines chartes BYOD mentionnent que le fait que *l'utilisateur peut à tout moment, moyennant un délai de 30 jours, décider de ne plus accepter la pratique du BYOD*.

32 MEIER, N 843 et les nombreuses réf. citées, p. 322.

une jurisprudence publiée (ATF 136 III 401[33]). Le Tribunal fédéral semble initier une distinction entre la révocation sur l'angle des droits de la personnalité et le contexte contractuel. Comme le relève Philippe Meier, la fidélité aux engagements pris paraît s'opposer à la révocation[34]. En réalité le contrat ne s'opposerait pas à la révocation, les engagements contractuels pris devant être respectés.

Le retrait du consentement pourrait être sanctionné contractuellement par l'allocation de dommages et intérêts[35] ou donner lieu au paiement d'une peine conventionnelle. La prudence commande donc de prévoir dans la charte BYOD que si le consentement de l'employé peut faire l'objet d'une rétractation en tout temps, celui-ci pourrait être tenu pour responsable en cas de dommage causé de ce fait à l'entreprise, par exemple en cas de résiliation en temps inopportun. Un tel cas pourrait se concrétiser si l'employé placé devant la nécessité de répondre à un appel d'offres dans un certain délai révoque son consentement ce qui engendrera la déconnexion des matériels du système d'information de l'entreprise et *a fortiori* un possible retard dans l'exécution de la tâche urgente à accomplir.

C. Horaires de travail

1. Protection de la personnalité du travailleur (art. 328 CO) et obligation de déconnexion

Une autre problématique que pose le BYOD en termes de droit du travail est la régulation des horaires de travail. L'employeur doit veiller à ce qu'il ne conduise pas à des usages de nature à modifier de manière substantielle les horaires de travail. En effet, par l'intermédiaire du BYOD, la société a au moins la possibilité de contrôler les excès de travail pendant le temps libre du salarié, ce qui peut avoir une incidence notamment sur les risques de dépassement des horaires légaux et la rétribution des heures supplémentaires. Le salarié pourrait se sentir obligé de répondre immédiatement aux mails, même pendant les vacances, les week-ends ou les jours fériés, ce qui suscite du stress et entrave la santé de l'employé[36]. La disponibilité continue étant l'un des avantages inhérents au BYOD, il devient presque impossible d'éteindre son *device*. L'employeur encourage

33 Dans cet arrêt le Tribunal fédéral considère qu'un engagement portant sur des biens de la personnalité ne faisant pas partie du cœur même de l'existence (nom, voix, image) ne peut pas être considéré comme révocable librement et en tout temps, car il porte avant tout sur des intérêts économiques.

34 MEIER, N 840 et les nombreuses réf. citées, p. 321.

35 Cf. MEIER, N 844, p. 323, qui évoque la possibilité de réclamer des dommages et intérêts lorsque la révocation intervient en temps inopportun au sens matériel, soit en l'absence de motifs sérieux.

36 MÖSSNER, § 1, p. 2.

également les salariés à utiliser les réseaux sociaux et procède à des analyses régulières pour vérifier que ses instructions sont respectées[37]. L'employeur est, sur le principe, en droit d'exiger une présence sur les réseaux sociaux (art. 321*d* CO)[38]. L'e-réputation d'une entreprise est désormais un facteur essentiel dans la communication des sociétés, de sorte que l'employeur souhaite obtenir de ses salariés qu'ils interagissent avec les clients et qu'ils deviennent en quelque sorte le porte-étendard de la marque. Les réseaux sociaux sont en effet un vecteur de publicité redoutable[39]. Précisons également que les risques qui viennent d'être exposés diffèrent notablement en fonction des catégories de personnels concernés.

Une récente étude américaine (Communication Technology : Implication for Work and Well-Being Report[40]) diligentée à l'initiative de l'American Psychological Association (avec Harris Interactive) a permis de mettre en exergue une connectivité quasi permanente, ainsi qu'une appréhension positive des salariés qui considèrent majoritairement que rester connecté est bon pour la productivité et l'équilibre[41]. La croyance actuelle dominante est donc que les nouvelles technologies présentent des avantages pour le travail, nonobstant le fait (que la majorité des sondés reconnaissent) que notre société est trop connectée. Selon cette étude :

- 53% des salariés interrogés vérifient les messages professionnels au moins une fois par jour le week-end ;
- 52% avant ou après le travail en cours de semaine ;
- 54% quand ils sont absents pour maladie ;
- 44% pendant les vacances.

Le psychologue David W. Ballard (correspondant du sondage à l'APA) rappelle que des temps d'arrêt sont nécessaires pour se remettre du stress au travail et éviter l'épuisement

---

37 Une entreprise internationale de travail temporaire organise des entretiens d'évaluation relatifs à cette utilisation d'Internet et des réseaux sociaux. Le montant des primes est impacté par les résultats de ces évaluations.

38 MANARA, p. 122.

39 FLUCKIGER, p. 842 : « *Facebook redéfinira aussi sûrement le standard de la sphère privée pour le XXI^e siècle que Kodak l'a fait, à la fin du XIX^e, pour tout le XX^e qui a suivi* ».

40 Accessible à cette adresse : http://www.apaexcellence.org/assets/general/2013-work-and-communication-technology-survey-final.pdf (consulté le 18 décembre 2013).

41 56% pensent que les technologies de communication permettent d'être plus productifs ; 53% qu'elles offrent plus de souplesse ; 56% reconnaissent qu'elles facilitent le travail ; 49% qu'elles ont un impact positif sur leurs relations avec les collègues, 71% qu'elles permettent de garder un contrôle sur ce qui se passe en dehors des heures ouvrables ; 69% qu'elles permettent de mieux faire cadrer leur emploi avec leur vie personnelle.

professionnel[42]. Cependant ces temps d'arrêt n'impliquent pas forcément une complète « désintoxication numérique ». C'est cependant sans compter différents effets collatéraux :

- 36% des répondants expliquent que ces technologies de communication augmentent leur charge de travail ;
- 34% qu'il est plus difficile d'arrêter de penser au travail ;
- 35% qu'il est plus difficile de faire une pause.

Dans ce contexte une violation de l'article 328 al. 2 du CO pourrait survenir[43]. Cet article prévoit un devoir général de protection de la personnalité du travailleur. L'alinéa 2 postule que l'employeur doit prendre, pour protéger la santé du travailleur, les mesures commandées par l'expérience, applicables en l'état de la technique, et adaptées aux conditions de l'exploitation, et cela dans la mesure où les rapports et la nature du travail permettent équitablement de l'exiger de lui. La portée de cet article dépasse de loin celle de l'article 28 du CC. Il impose à l'employeur non seulement le respect de la personnalité du salarié, mais également la prise de mesures concrètes en vue de la protection de sa vie, de sa santé et de son intégrité corporelle[44].

L'employeur doit ménager l'intégrité de ses employés en s'abstenant de leur demander des efforts excessifs et de les charger de travaux pouvant porter atteinte ou mettre en danger leur santé[45]. Dans un contexte d'essor technologique constant, les atteintes à la santé sont amenées à progresser. À titre exemplatif, on peut évoquer un stress extrême généré par l'impossibilité de déconnecter[46], une surcharge de travail ou encore un épuisement professionnel (burnout)[47]. Le salarié pourrait également développer un syndrome de cyberdépendance (ou cyberaddiction), dont l'employeur serait alors responsable, à tout le moins partiellement. Il y a donc objectivement motif à intervention

42 http://www.santelog.com/news/neurologie-psychologie/work-addict-en-conge-la-moitie-des-salaries-reste-connectee_11043_lirelasuite.htm (consulté le 18 décembre 2013).

43 REUTTER/KLAUS, p. 161.

44 STAUDER, N 2 ad art. 328 CO.

45 Message 1967, p. 354 ; DUNAND, N 14 ad art. 328 CO, p. 275.

46 La difficulté de se déconnecter est amplifiée par les nouveaux outils d'information et de communication de sorte que l'on évoque l'esclavagisme numérique qui se traduit par des comportements déviants toujours plus intrusifs : je vous envoie un mail ; en cas d'absence de réponse dans un délai que je considère unilatéralement comme convenable, je renvoie un mail et/ou j'appelle, respectivement je vous dérange sur votre portable…

47 Pour de plus amples informations, cf. LETSCH, N 51 ss.

de la part de l'employeur, ces conséquences devant être qualifiées désormais de notoires, dès lors que des programmes thérapeutiques sont diligentés pour y remédier[48].

Aux fins d'éviter de tels risques dans le cadre du BYOD, il pourrait être envisagé de bloquer l'accès à l'espace dédié aux utilisations professionnelles en dehors des heures travaillées et pendant les temps non travaillés (week-end, jour férié, vacances, etc.). L'introduction d'une obligation de déconnexion[49] par l'employeur est également un sujet actuel et pertinent[50]. Ne faudrait-il pas prévoir des temps de repos automatisés, respectivement des périodes où les salariés ne sont pas connectés à l'infrastructure informatique de l'entreprise ? Tout comme par le passé, il était conseillé de faire une pause après avoir regardé de manière soutenue la télévision, la question se pose légitimement en matière de BYOD. En sus de la prohibition absolue de se connecter durant certaines périodes (week-end, jours fériés, vacances), l'employeur ne devrait-il pas imposer une déconnexion de l'ordre de 5 minutes après deux heures ininterrompues de travail au moyen des outils informatiques de l'entreprise ? Il s'agirait d'un premier pas intéressant qui mérite réflexion et va très certainement connaître des développements, à l'aune du nombre de personnes actuellement soignées pour leur addiction.

2. Vacances (article 329*a* CO et 329*d* al. 2 CO)

Les vacances dont la durée est fixée à l'article 329*a* du CO doivent être consacrées au repos du salarié, ce que confirme le texte de l'article 329*d* al. 2 CO qui prohibe le remplacement de celles-ci par des prestations en argent ou d'autres avantages. Cette dernière disposition est de droit semi-impératif en vertu de l'article 362 al. 1 CO. À défaut, le but des vacances ne pourrait être atteint. Il en va de même si l'employé utilise de manière continue son appareil privé pour accomplir des tâches professionnelles durant les vacances. L'employeur qui tolérerait une telle activité professionnelle durant les vacances prendrait le risque de devoir les octroyer une nouvelle fois, respectivement de voir cette période de vacances être transformée en indemnité au terme du contrat de travail[51]. Ainsi que cela a été exposé précédemment, la solution la plus simple consiste à bloquer l'accès à l'espace dédié aux utilisations professionnelles pendant les vacances.

---

48 Pour un exemple de test visant à détecter une cyber-dépendance : http://www.cliniquebelmont.ch/sites/default/files/02-belmont_05-12-pdf_deceler-cyber.pdf ; le site infoset.ch recèle un très grand nombre d'informations consacrées à ce sujet : http://www.infoset.ch/f/dependances/cyberdependance/ (consultés le 18 décembre 2013).

49 Voir CAUVIN.

50 Voir RAY.

51 ATF 131 III 451, consid. 2.2, JdT 2006 II 129 ; REUTTER/KLAUS, p. 162.

3. Travail du jour et travail du soir (art. 10 LTr) ; interdiction de travailler la nuit (art. 16 LTr) ; dérogation à l'interdiction de travailler la nuit (art. 17 LTr)

Les règles relatives au travail du jour et travail du soir figurent à l'article 10 de la Loi fédérale sur le travail du 13 mars 1964 (LTr)[52]. Selon l'alinéa 1er de cette disposition légale : il y a travail de jour entre 6 heures et 20 heures, et travail du soir, entre 20 heures et 23 heures. Le travail de jour et le travail du soir ne sont pas soumis à autorisation. Le travail du soir peut être introduit par l'employeur après audition de la représentation des travailleurs dans l'entreprise ou, à défaut, des travailleurs concernés. L'occupation des travailleurs est interdite en dehors des limites du travail de jour et du travail du soir (article 16 LTr). Les dérogations à l'interdiction de travailler la nuit sont soumises à autorisation (art. 17 LTr).

L'employeur doit accorder une majoration de salaire de 25% au moins au travailleur qui effectue un travail de nuit à titre temporaire (art. 17*b* LTr), peu importe à cet égard qu'une autorisation ait été obtenue ou non[53]. Il s'agit là d'une prescription de droit impératif, qui prévaut sur le droit conventionnel : en d'autres termes, l'employeur est tenu de verser au travailleur ce supplément de salaire de 25% pour le travail de nuit à caractère temporaire, même lorsqu'un pourcentage inférieur a été fixé par contrat. Sont à l'inverse applicables les conditions d'un contrat qui prévoit un supplément de salaire supérieur à 25%, puisqu'il respecte d'ores et déjà le minimum légal[54].

Les dérogations à l'interdiction de travailler le dimanche sont soumises à autorisation (art. 19 al. 1 LTr). L'employeur accorde dans ce cas une majoration de salaire de 50% au travailleur (art. 19 al. 3 LTr) ainsi qu'un repos compensatoire (art. 20 al. 2 LTr).

L'employeur qui tolèrerait que des prestations professionnelles soient exécutées durant la nuit ou le dimanche prendrait le risque de devoir payer une majoration de salaire en sus d'être condamné pour ne pas avoir respecté la durée du travail ou du repos, soit n'avoir pas sollicité et/ou obtenu une autorisation (art. 59 al. 1 let. b LTr) à une peine pécuniaire de 180 jours-amende (art. 61 alinéa 1 LTr) en cas de comportement intentionnel. Pour éviter de tels écueils, les remarques émises au point précédent valent *mutatis mutandis*[55].

52 RS 822.11.
53 OFK-MÜLLER (2009), Kommentar ArG 17*b* Abs. 1.
54 SECO, ad article 17*b* LTr.
55 REUTTER/KLAUS, p. 163.

D. Frais professionnels (art. 327 al. 2 CO, 327*a* CO)

D'ordinaire, l'employeur fournit au travailleur les instruments de travail et les matériaux (art. 327 al. 1 CO). Si d'entente avec l'employeur le travailleur fournit lui-même ces instruments de travail ou ces matériaux, il est indemnisé convenablement, sauf accord ou usage contraire (art. 327 al. 2 CO). La première condition est donc que l'employeur ait été informé de la démarche du salarié, respectivement qu'il l'ait tolérée.

L'article 327*a* al. 1 du CO prévoit quant à lui que l'employeur est tenu de rembourser au travailleur tous les frais imposés par l'exécution du travail et, lorsque le travailleur est occupé en dehors de son lieu de travail, les dépenses nécessaires pour son entretien. Il s'agit d'une disposition semi-impérative à laquelle il ne peut être dérogé au détriment du travailleur (art. 362 al. 1 CO).

Les coûts liés aux communications professionnelles doivent être assumés par l'employeur pour autant qu'il s'agisse de dépenses nécessaires (art. 327*a* al. 1 CO). En cas de litige, c'est le travailleur qui devra apporter la preuve du bien-fondé et de l'étendue des frais dont le remboursement est sollicité[56]. Les exigences en cette matière ne sauraient être trop élevées.

L'employeur devra également participer à la prise en charge des coûts d'acquisition du matériel et à ses coûts d'amortissement (art. 327 al. 2 CO). Un accord contraire est réservé, ce qui signifie qu'il est toujours possible de convenir d'une clé de répartition en faveur de l'employeur, voire d'une absence d'indemnisation. Cette possibilité d'économies peut évidemment inciter l'employeur à introduire le BYOD. Un calcul schématique est de ce point de vue complexe, car il dépend de nombreux facteurs (prix d'acquisition subventionné, valeur résiduelle en fonction de la durée de possession antérieure à l'introduction du BYOD, responsabilités assumées par le salarié dans l'entreprise et nécessité objective d'usage accru...).

En ce qui concerne les abonnements téléphoniques (comprenant désormais des forfaits de données), la question se pose de savoir si l'article 327*a* CO trouve ou non application. Une solution pragmatique[57] pourrait consister à prendre en charge partiellement les coûts de l'abonnement, par exemple en offrant un abonnement de base permettant d'accomplir les tâches du cahier des charges du salarié. On pourrait imaginer que pour les cadres dirigeants, dont les besoins sont logiquement plus intenses, un forfait plus étendu soit offert. Il s'agit également d'un moyen de fidéliser et de récompenser le salarié. Dans quelques années, le téléphone et les prestations y relatives pourraient s'avérer faire partie

56 ATF 131 III 439, consid. 5, JdT 2006 I 35.
57 BIRKHÄUSER/HADORN, p. 202.

des conditons d'engagement de tout collaborateur. La tendance est donc à offrir plus de prestations aux employés. Si la concurrence dans un secteur d'activité est féroce, cette question ne se posera plus guère en pratique dès lors que cet effort consenti participera à la stratégie d'engagement des meilleurs collaborateurs. La diminution du coût des forfaits téléphoniques et de données réduira également l'acuité de la problématique de répartition, laquelle n'est du point de vue légal pas encore tranchée. Finalement, l'employeur pourra déduire, au titre de ses charges, l'investissement ainsi consenti, alors que tel ne sera pas le cas du salarié.

Finalement, au terme des rapports de travail, l'employeur pourrait être tenté de solliciter une compensation pour avoir participé à l'acquisition et/ou l'amortissement de l'appareil privé. *De facto*, à l'aune de la durée de vie réduite de tels *devices*, cela paraît technologiquement et économiquement sans intérêt, même si légalement une telle clause pourrait figurer dans une charte BYOD en vertu de l'article 327 alinéa 2 CO.

E. Responsabilité en cas de dommage ou de perte (art. 321*e* CO)

Dans l'hypothèse d'un vol ou d'un dommage causé à l'appareil privé, se posera logiquement la question de savoir qui prend en charge les coûts qui en résulteront, comme les coûts de réparation ou de remplacement. Par analogie, on peut appliquer les règles relatives à l'utilisation d'un véhicule privé, figurant à l'article 327*b* du CO. Selon la jurisprudence[58], les dommages matériels occasionnés dans le cadre de l'activité professionnelle doivent être assumés par l'employeur, dans la même mesure où celui-ci répond d'un accident de travail. Cela signifie concrètement que si l'appareil est volé lors d'une période de vacances durant laquelle l'employé n'a pas le droit de travailler ou ne peut le faire en raison des mesures techniques déjà évoquées, le remplacement pourrait être à sa charge. Une solution satisfaisant les intérêts des deux parties pourrait consister à assurer l'appareil en lieu et place de verser une indemnité pour son amortissement ou à prolonger la garantie. Le contrat d'assurance, respectivement la garantie ne couvrirait certes pas toutes les hypothèses évoquées, mais il permettrait déjà de limiter quelque peu les risques.

Selon l'article 321*e* CO, le travailleur répond du dommage qu'il cause à l'employeur intentionnellement ou par négligence. Il ne peut être dérogé à cet article au détriment de l'employé (art. 362 al. 1 CO). La limite s'agissant de la responsabilité du travailleur consiste à ne pas lui faire supporter le risque économique de l'entreprise qui incombe à

58 RJJ 1996, p. 246 ; ZR 87, n° 73.

l'employeur. L'appareil en tant que tel n'aura que rarement une valeur à neuf supérieure à CHF 1'000.-. La valeur résiduelle devrait de surcroît être prise en considération, ce qui réduit encore le dommage. Il faut certes tenir compte du temps consacré à réinstaller les solutions logicielles, mais on imagine mal que le dommage total puisse dépasser quelques milliers de francs. D'autre part, le fardeau de la preuve incombant à l'employeur[59], il sera souvent difficile de déterminer quand et comment le dommage ou la perte sont réellement intervenus, sauf à géolocaliser en permanence les collaborateurs ce qui est formellement proscrit. Une fois encore, à moins d'un comportement intentionnel ou gravement négligent visant à causer manifestement un dommage à l'employeur (collaborateur qui omet d'enregistrer le résultat de son travail soit un appel d'offres important dans la partie consacrée aux documents professionnels et qui bien qu'en sachant l'importance de cet appel d'offres le prête à un tiers pour que ses enfants puissent jouer tout en sachant qu'à un jeune âge l'appareil peut être endommagé…), il paraît difficile de faire supporter le dommage à l'employé. De tels cas devraient donc demeurer exceptionnels.

Relevons également le fait qu'une campagne de sensibilisation est susceptible d'engendrer une diminution drastique de ce risque. Le site de la Fédération française des télécoms est à cet égard un excellent exemple[60] des conseils qui peuvent être dispensés utilement.

III. Règles applicables en matière de protection des données

A. Atteintes à la personnalité de tiers

Le risque principal consiste pour l'employeur et ses salariés[61] à porter atteinte à l'intégrité informationnelle d'un tiers[62] lors d'un traitement de données, soit par exemple un partenaire commercial ou un client[63]. Il convient de déterminer *in concreto* si la personne concernée subit une telle atteinte. L'article 12 al. 2 de la Loi fédérale sur la protection des données du 19 juin 1992 (LPD)[64] contient toutefois une liste non

59 JAR 1999, p. 292 ; SARB 1999, p. 647.
60 http://www.mobilevole-mobilebloque.fr (consulté le 18 décembre 2013).
61 Cf. art. 319 al. 1 CO.
62 MEIER, N 1531, p. 705.
63 MÖSSNER, § 2.2, p. 9.
64 RS 235.1.

exhaustive de cas dans lesquels l'atteinte est présumée de manière irréfragable (fiction)[65]. Nous allons examiner dans le détail quelques situations pouvant engendrer de telles atteintes.

1. Violation du principe de sécurité (art. 7 al. 1 LPD, art. 8 et 9 OLPD)

L'article 7 alinéa 1er LPD intitulé *Sécurité des données* prévoit que les données personnelles doivent être protégées contre tout traitement non autorisé par des mesures organisationnelles et techniques appropriées. On ne saurait exiger une protection absolue, car il est impossible de se prémunir contre toutes les éventualités. Ce principe est concrétisé à l'article 8 de l'Ordonnance relative à la Loi fédérale sur la protection des données (OLPD)[66] qui prévoit une prise en considération de la situation globale pour déterminer que les sont les mesures organisationnelles et techniques appropriées. La question de savoir si les moyens financiers doivent être pris en considération est contestée[67], mais comme le relève avec pertinence Henrike Mössner[68], cela importe en définitive peu dès lors que les moyens financiers peuvent encore être invoqués comme moyens justificatifs dans le cadre de la pesée des intérêts ultérieure.

Un *update* des mesures de sécurité est évidemment nécessaire et il devrait intervenir tous les ans, sauf circonstances extraordinaires, c'est à dire par exemple une adaptation des normes légales[69].

L'article 9 al. 1 OLPD prévoit quant à lui différentes mesures particulières, techniques et organisationnelles, pour sécuriser les données, avec huit objectifs nommément cités qui doivent servir de *fil rouge* aux entreprises. Le contrôle des supports de données personnelles y est expressément mentionné (art. 9 al. 1 let. b) en ces termes : « *les personnes non autorisées ne peuvent pas lire, copier, modifier ou éloigner des supports de données* ».

Dans le cas du BYOD, le risque majeur est lié à une impossibilité de sécuriser de manière absolue les données figurant sur les appareils privés[70]. Pour illustrer ce propos, précisons que le code PIN[71] peut être craqué avec des outils disponibles gratuitement sur

65 MEIER, N 1531, p. 705.
66 RS 235.11.
67 ATAF A-4467/2011 du 10 avril 2012, consid. 9.
68 MÖSSNER, § 2.2.2.1, p. 11.
69 ATAF A-4467/2011 du 10 avril 2012, consid. 9.
70 Pour des exemples de sécurisation : EYNARD, § 2 (les outils techniques), p. 335.
71 Soit *Personal Identification Number*, il s'agit d'un code comportant au moins 4 chiffres utilisé sur un téléphone mobile et qui protège la carte SIM contre toute utilisation non autorisée.

Internet en 15 à 20 minutes[72]. L'empreinte introduite par Apple n'a constitué une sécurité effective que durant une seule journée. Le Secrétariat général de la défense et de la sécurité nationale et l'Agence nationale de la sécurité des systèmes d'informations de la France (ANSSI) ont émis le 19 juin 2013 une Note technique intitulée : « *Recommandations de sécurité relatives aux ordiphones* »[73]. Parmi les 21 recommandations émises, certaines s'appliquent aux *devices* :

- configurer une durée d'expiration du mot de passe de 3 mois au maximum ;
- configurer le verrouillage automatique de terminal au bout de 5 minutes au maximum ;
- si le terminal contient des informations sensibles[74], exiger un mot passe fort en remplacement des méthodes de verrouillage par défaut ;
- limiter le nombre de tentatives de déverrouillage, puis configurer un temps de blocage de plus en plus long ainsi qu'un effacement automatique après une dizaine de tentatives ayant échoué ;
- ne jamais laisser un terminal sans surveillance ;
- ne pas brancher le terminal à un poste de travail non maîtrisé ou à un quelconque périphérique qui ne soit pas de confiance ;
- interdire l'utilisation du magasin d'applications par défaut, ainsi que l'installation d'applications non explicitement autorisées par l'entreprise ;
- les applications installées doivent avoir fait l'objet d'une étude de réputation avant qu'une autorisation de déploiement soit délivrée ;
- l'accès au service de géolocalisation doit être interdit aux applications dont les fonctions liées à la position géographique ne sont pas utilisées ;
- mettre à jour régulièrement les applications déployées ;
- les interfaces sans-fil (Bluetooth et WiFi) ou sans contact (NFC par exemple) doivent être désactivées lorsqu'elles ne sont pas utilisées ;
- désactiver systématiquement l'association automatique des points d'accès WiFi configurés dans le terminal afin de garder le contrôle sur l'activation de la connexion sans-fil ;

---

72 Voir NESTENREKO.

73 Le document est disponible à cette adresse : http://www.ssi.gouv.fr/fr/bonnes-pratiques/recommandations-et-guides/securite-des-solutions-de-mobilite/recommandations-de-securite-relatives-aux-ordiphones.html (consulté le 18 décembre 2013).

74 Ce qui est le cas dans le domaine du BYOD.

- éviter autant que faire se peut de se connecter à des réseaux sans fil inconnus et qui ne sont pas de confiance ;
- crypter le stockage amovible et le stockage interne du terminal ;
- mettre à jour régulièrement le système d'exploitation ;
- etc.

L'ANSSI expose en ces termes les risques inhérents : « En tout état de cause, il est illusoire d'espérer atteindre un haut niveau de sécurité avec un ordiphone ou une tablette ordinaire, quel que soit le soin consacré à son paramétrage ». Les révélations d'Edward Snowden[75] ont engendré, en sus d'une prise de conscience collective, des offres de téléphones sécurisés, dont il faut bien admettre qu'elles ne sont et ne seront jamais totalement satisfaisantes[76], à l'aune de la surveillance étatique et privée notamment. Caspar Bowden[77], l'ancien Chief Privacy Adviser de Microsoft, a mis en exergue dans une étude (commandée par la commission des libertés civiles, de la justice et des affaires intérieures du Parlement européen) les risques des programmes de surveillance des États-Unis et leurs effets sur les droits fondamentaux des citoyens de l'UE[78]. Ces risques, désormais connus de tous, font partie de ceux qui doivent être intégrés à l'analyse.

Nicole Beranek Zanon propose à cet égard l'élaboration d'une matrice complète qui tient compte du type de données, des fichiers concernés, ainsi que de la classification des données au sein de l'entreprise[79]. Henrike Mössner expose trois cas d'utilisation du BYOD et après analyse met en exergue les mesures appropriées à adopter[80]. Un concept détaillé doit être élaboré par l'employeur, comprenant une analyse de risques et de vulnérabilités spécifiquement de l'outil privé. Le concept de mobilité nécessaire des données est évoqué en ce sens qu'il convient de s'interroger sur la nécessité pour les données de quitter la sphère physique de l'entreprise. Y a-t-il encore la possibilité d'utiliser des systèmes de Data Loss Prevention (DLP) ? Il s'agit d'un ensemble de

75 Pour un résumé : http://lexpansion.lexpress.fr/high-tech/prism-l-espionnage-du-web-a-grande-echelle_389722.html ; http://fr.wikipedia.org/wiki/Edward_Snowden (consultés le 18 décembre 2013).

76 Voir NESTENREKO ; LEBLAL.

77 http://en.wikipedia.org/wiki/Caspar_Bowden (consulté le 18 décembre 2013).

78 Cette étude se penche sur la portée de la surveillance que les Etats-Unis peuvent exercer en vertu de l'amendement de 2008 de la loi FISA, ainsi que sur les pratiques des autorités américaines dans ce contexte, lesquelles ont d'importantes conséquences sur la souveraineté de l'UE sur les données qu'elle produit et sur la protection des droits des citoyens européens : http://www.europarl.europa.eu/RegData/etudes/note/join/2013/474405/IPOL-LIBE_NT(2013)474405_FR.pdf (consulté le 18 décembre 2013).

79 BERANEK ZANON, N 15.

80 MÖSSNER, § 2.2.2.2, p. 16 ss.

techniques de protection contre la fuite d'informations[81]. Comme dans le contexte du BYOD des données privées peuvent et vont très certainement circuler dans le réseau privé de l'entreprise, une telle collecte de données personnelles apparaît disproportionnée à certains auteurs[82]. Le problème est aigu dès lors que les solutions BYOD du marché peuvent, techniquement, comporter des fonctionnalités de Data Loss Prevention[83]. La question demeure donc ouverte.

Il convient donc *a minima* de mettre en place une politique de sécurité et de formaliser dans une charte les obligations liées à cette question topique visant à garantir la disponibilité et l'intégrité des données de l'entreprise. Une campagne de sensibilisation constituerait un complément utile à ces mesures normatives, la prévention demeurant la meilleure arme de défense. Le principe de sécurité des données s'appliquera en effet avec plus de rigueur dès lors que le BYOD, par nature, accroît le risque de porter atteinte aux intérêts de tiers. L'implémentation du processus alors que les aléas sont désormais connus constitue selon certains déjà une violation du principe de sécurité des données[84].

2. Violation du principe de la bonne foi : perte de données (Data Breach) et devoir d'information (art. 4 al. 2 LPD)

Cette clause générale figure à l'article 4 alinéa 2 LPD qui fait le lien en matière de protection des données entre la protection de la personnalité (art. 28 CC) et le principe de la bonne foi ancré à l'article 2 CC[85]. Si une entreprise prend l'engagement de détruire des dossiers de candidature des personnes qui n'ont pas été choisies et ne le fait pas, elle viole ce principe. La violation de ce principe a pour conséquence de faire présumer l'illicéité du traitement (art. 12 al. 2 let. a, art. 15 et art. 25 LPD), sous réserve des motifs justificatifs (art. 13 LPD)[86].

Des exemples de perte de données sont évoqués au quotidien par les médias[87]. Certains cas ont provoqué des remous jusque dans les milieux politiques, avec des conséquences importantes en termes de réputation d'entreprise. Le Sonygate en est un exemple

81 Pour de plus amples informations : http://fr.wikipedia.org/wiki/Data_Loss_Prevention (consulté le 18 décembre 2013).
82 MÖSSNER, § 2.2.2.3, p. 19.
83 CROCHET-DAMAIS.
84 MÖSSNER, § 2.2.2.3, p. 18.
85 MEIER, N 647, p. 264.
86 MEIER, N 660, p. 267.
87 Pour un exemple récent : http://www.bbc.co.uk/news/technology-25213846 (consulté le 18 décembre 2013) ; plus de 2 millions d'accès à des comptes pour des sites comme Facebook, Google et Yahoo ! ont été volés dans le monde entier et publiés sur un site Internet.

marquant[88]. L'intégrité et l'accès aux données de 77 millions d'abonnés du PSN (Playstation Network) et de son service de musique en streaming Qriocity ont été gravement compromis. En Suisse, 450'000 personnes ont été concernées. Suite à une intrusion, des données personnelles ont été, selon Sony, volées (adresse de courriel, sexe, pseudonyme utilisé, données de la carte de crédit, date de naissance, mot de passe, etc.).

Y aurait-il dans le cadre du BYOD une obligation d'informer (Data Breach Notification) de la part de l'employeur fondée sur principe de la bonne foi inscrit à l'article 4 al. 2[89] de la LPD ? Comme le mentionne Henrike Mössner[90], on pourrait imaginer la perte de données clients comportant des indications de blocage pour des communications marketing. Si ces clients devaient être ensuite contactés à cette fin, cela pourrait anéantir la relation de confiance, dans l'hypothèse où la perte de données ne leur a pas été annoncée. À ce jour, la question du devoir d'annonce n'est pas tranchée dans notre pays[91]. L'argumentaire développé par Henrike Mössner[92] selon lequel un devoir de notification paraîtrait opportun dans le cas où l'on a affaire à un incident relatif à la sécurité des données qui entraîne au moins un niveau de risque moyen pour la personne concernée de subir un préjudice est convaincant. La multiplication des notifications pourrait alarmer inutilement les personnes concernées et, à terme, créer une banalisation, avec pour conséquence l'absence de prise en considération de l'existence d'un danger réel. L'exemple cité de l'envoi d'un mail professionnel depuis un appareil privé via un réseau Wi-Fi non sécurisé en est une illustration parfaite, puisque dans une telle hypothèse si l'entreprise en est informée, elle devra impérativement signaler le risque de divulgation de données. La condition objective est donc la connaissance par l'employeur d'une faille de sécurité. À défaut, il n'y pas d'obligation d'annonce. Par contre, le fait de devoir informer les partenaires de l'entreprise de l'utilisation du BYOD nous paraît excessif. L'introduction de ce devoir d'information active pourrait entraver les processus commerciaux en suscitant des craintes qui n'auraient peut-être pas lieu d'être si le BYOD est introduit avec les mesures de sécurité adéquates. Le problème pourrait également être réglé à l'envers : toute société qui possède des données sensibles devrait intégrer dans ses contrats avec ses partenaires une obligation d'information relativement au BYOD, ainsi qu'une obligation d'annonce en cas de *data breach*, le tout avec pour corollaire une clause pénale qui trouverait application en cas de défaut.

88 Cf. pour de plus amples informations, CHABOT, § IV, p. 6.

89 Qui prévoit que le traitement des données doit être effectué conformément au principe de la bonne foi et de la proportionnalité.

90 MÖSSNER, § 2.2.3.1, p. 20.

91 Cf. notamment EBNETER, N 11 ss et N 16 ss.

92 MÖSSNER, § 2.2.3.1, p. 23.

3. Communication transfrontière de données et exemple du *Cloud* (art. 3 let. f, 6 et 10*a* LPD)

La communication transfrontière des données est régie par l'article 6 LPD. La notion de communication est quant à elle définie à l'article 3 let. f LPD : « *le fait de rendre des données personnelles accessibles, par exemple en autorisant leur consultation*[93]*, en les transmettant ou en les diffusant*[94] ». Il n'y pas communication lorsque le tiers a déjà connaissance des données auparavant ; en revanche, lorsque le détenteur de données lui octroie un accès plus large aux données déjà en sa possession, on est bien en présence d'une communication[95].

L'employé est un tiers au sens de cette disposition dès lors qu'il accède à ses mails professionnels lors de la synchronisation du courrier électronique le soir ou pendant le week-end, alors qu'il se trouve dans un cadre privé[96]. Comme c'est lui qui déclenche le transfert de données, on imagine difficilement qu'il puisse être considéré qu'il ne s'agit pas d'une communication au sens de l'article 3 let. f LPD.

La question de savoir si l'employé qui, par exemple, relève ses courriels professionnels lors de vacances à l'étranger, engendre une communication transfrontière selon 6 LPD est débattue[97]. Comme l'employé ignore le contenu de ces courriels, il y a bien une communication de données et l'on ne saurait invoquer un accès dit d'usage personnel[98]. L'utilisation par un membre de la famille de l'appareil privé ne constitue pas une communication passive en l'absence de volonté autre que celle d'accéder aux informations personnelles[99].

Quid du *Cloud computing*[100] ? Le *Cloud computing* est un modèle permettant l'accès aisé et à la demande à un ensemble de ressources de calculs configurables pouvant être rapidement provisionnées et mises à disposition avec un effort d'administration ou des interactions avec le fournisseur de services minimes.

Les employés synchronisent régulièrement leurs données personnelles (mails, carnets d'adresse, calendrier, photos, vidéos, documents, musique, etc.) par l'intermédiaire de

93 Communication passive.
94 Communication active.
95 MEIER, N 545, p. 237.
96 ATAF A-4467/2011 du 10 avril 2012, consid. 6.3.1.
97 MÖSSNER, § 2.2.4.1, p. 27.
98 WALTER, p. 119.
99 ATAF A-4467/2011 du 10 avril 2012, consid. 6.2 et 6.3.
100 FANTI, p. 74-77.

tels services. Il paraît donc difficile de prohiber leur utilisation, sous peine de provoquer l'incompréhension et l'ire des salariés, à l'aune des avantages que cela leur procure.

Fondamentalement, le traitement de données personnelles découlant de l'utilisation des services de *Cloud* computing relève du traitement de données par un tiers au sens de l'article 10*a* LPD. La première condition est que le traitement par un tiers est autorisé pour autant que la loi ou une convention le prévoie. En sus, différentes conditions sont émises, dont il résulte des obligations positives ténorisées dans les conseils que voici.

Le Préposé fédéral à la protection des données et à la transparence recommande[101] :

- de n'effectuer que des traitements que le mandant peut effectuer lui-même (art. 10*a* al. 1 let. a LPD) ;
- de vérifier qu'aucune obligation légale ou contractuelle de garder le secret ne proscrive un tel traitement (secret professionnel, bancaire, médical, etc.) ;
- de s'assurer *in concreto* que le tiers assure effectivement la sécurité des données (art. 10*a* al. 2 LPD) ; il ne suffit donc pas de se fier aux assurances du prestataire, mais des vérifications concrètes, régulières, et *in situ* doivent être opérées (cf. 7 LPD, 8 ss et 20 ss OLPD) ; le prestataire doit protéger les données contre les risques suivants : destruction accidentelle ou non autorisée ; perte accidentelle ; erreurs techniques ; falsification, vol ou utilisation illicite ; modification, copie, accès ou autre traitement non autorisés ;
- de s'assurer en cas de communication de données à l'étranger de l'existence d'un niveau de protection adéquat (cf. art. 6 LPD), la preuve de la pertinence et de l'efficience des précautions prises incombant à celui qui transfère les données à l'étranger ;
- de s'assurer de l'accès en tout temps aux données (art. 8 LPD) et du droit d'effacer ou de rectifier les données (art. 5 LPD) ; le fait d'ignorer où ces données sont traitées n'exonère pas l'utilisateur de ces services de ces obligations légales.

Ainsi la première démarche à accomplir est de solliciter des salariés pour qu'ils indiquent si une synchronisation par le biais d'un service *Cloud* intervient s'agissant de leurs données privées. En exposant les risques et en détaillant les obligations figurant à l'article 6 LPD, l'employeur devrait être à même de convaincre ses salariés du bien-fondé d'une démarche, qui a sommes toutes également pour but de protéger leurs intérêts. Des conseils pourraient ainsi être dispensés même pour les données privées, ce qui permettrait d'accroître le niveau général de sécurité dans l'entreprise.

---

[101] Explications concernant l'informatique en nuage (*Cloud computing*), disponible à cette adresse : http://www.edoeb.admin.ch/themen/00794/01124/01768/index.html ?lang=fr (consulté le 18 décembre 2013).

Le problème se pose avec une acuité particulière s'agissant des États-Unis, pays pour lequel une réglementation spécifique existe. Un accord-cadre intitulé « U.S. – Swiss Safer Harbor Framework » garantit une protection adéquate au sens de l'article 6 al. 1 let. a LPD[102]. Il s'agit d'un engagement bilatéral qui simplifie le transfert des données personnelles des entreprises établies en Suisse vers des entreprises aux États-Unis. Toutefois, le Safe Harbor ne s'applique qu'aux entreprises américaines qui sont soumises à l'autorité de l'US Federal Trade Commission ou de l'USD Department of Tansportation[103]. Seul le traitement des données de personnes physiques y est réglé, les données du personnel et les données traitées manuellement n'étant couvertes que pour autant qu'elles soient mentionnées dans la certification de l'entreprise[104]. Concrètement, cela signifie que différentes vérifications devront être opérées nonobstant le fait qu'une entreprise américaine se soit soumise à cet accord. Cette prudence doit encore être accrue en cas de délégation du traitement de données comme cela est le cas en matière de *Cloud computing*.

Différents auteurs évoquent la nécessité de la conclusion d'un contrat spécifique entre l'entreprise et le fournisseur du service *Cloud* pour respecter les réquisits de l'article 6 al. 1 LPD[105]. Il apparaît toutefois difficile d'obtenir des principaux fournisseurs (Google, Amazon, Microsoft, Apple, etc.) des aménagements contractuels à moins d'être une multinationale et de représenter un intérêt économique notable pour le cocontractant. D'expérience, jamais il n'a été possible d'obtenir l'inclusion de telles clauses (interdiction de communiquer des données à des sous-traitants, possibilité d'exercer le droit d'accès pour le titulaire…). Émettre de telles exigences est actuellement illusoire. Les scandales à répétition suite aux révélations d'Edward Snowden vont engendrer des pertes massives pour l'industrie américaine du *Cloud*[106], laquelle va probablement être plus encline à négocier des garanties supplémentaires. À l'heure où ces lignes sont écrites, dans la cadre d'une négociation pour un acteur majeur suisse, il n'a pas été possible d'obtenir un quelconque aménagement de la part de Google pour ses services *Cloud*.

Il est donc, à l'aune des exigences légales précitées, douteux que la synchronisation avec des services *Cloud* dont les données sont stockées aux USA puisse s'avérer licite. Il sera,

---

102 Pour de plus amples informations, cf. le site du PFPDT : http://www.edoeb.admin.ch/datenschutz/00626/00753/00970/index.html?lang=fr (consulté le 18 décembre 2013).

103 MEIER, N 1136, p. 459.

104 MEIER, N 1136, p. 459.

105 MÖSSNER, § 2.2.4.2 et les réf. citées, p. 31.

106 Selon l'ITIF (Information Technology & Innovation Foundation), elles oscilleront entre 21.5 et 35 milliards de dollars durant les trois prochaines années.

dans ces conditions, préférable de privilégier des solutions nationales ou européennes, ce d'autant que pour une petite entreprise, les services offerts sont tout à fait satisfaisants.

En définitive, en l'absence de contrat avec l'exploitant du service de *Cloud*, le maître du fichier pourrait ne pas remplir son devoir de diligence ce qui rendra la communication illicite. Dans le cadre de la synchronisation des appareils privés via un tel service, les exigences seront encore plus élevées (respect des principes généraux du traitement). Le transfert de grandes quantités de données dans le *Cloud* s'avère disproportionné (art. 4 al. 2 LPD), car le maître du fichier doit limiter la communication au strict minimum. C'est à vrai dire, la problématique la plus aiguë en cette matière dès lors que sa résolution dépend d'efforts contractuels du fournisseur de services *Cloud* que les entreprises américaines ne sont pas prêtes à consentir. Le seul expédient est donc de se tourner, pour l'heure, vers des sociétés ayant leur siège au sein de l'UE, respectivement en Suisse.

4. Difficultés engendrées par l'exercice d'un droit d'accès (art. 8 LPD)

L'exercice du droit d'accès est formalisé à l'article 8 LPD qui constitue une garantie fondamentale de veiller au respect de la sphère privée qui figure dans la Constitution fédérale (art. 13 Cst.). Son exercice n'est pas subordonné à une atteinte à la personnalité[107]. Pour éviter de devoir répondre dans le délai légal de 30 jours (art. 1 al. 4 OLPD), l'employeur pourrait invoquer l'existence d'un intérêt privé prépondérant (art. 9 al. 4 LPD), par exemple en matière de BYOD, le coût exorbitant du tri entre les données privées et professionnelles lié à son absence d'accès aux données figurant sur l'appareil privé[108]. Dans la mesure où il s'agit d'un droit fondamental, cet argument de défense paraît peu solide, ce d'autant que les solutions actuelles en matière de BYOD permettent un tri initial lors de la mise en service. Il contrevient également à l'article 9 al. 2 OLPD qui prescrit à l'employeur d'organiser ses fichiers de manière à pouvoir en extraire les données nécessaires.

L'employeur prendrait un risque considérable s'il refusait indûment de déférer à une requête d'accès sur le plan réputationnel notamment. L'article 34 al. 1 let. a LPD pourrait trouver application en cas de plainte avec pour corollaire une condamnation pénale à une amende jusqu'à 10'000 francs.

107 MEIER, N 968, p. 362.
108 MÖSSNER, § 2.2.5, p. 32.

En matière de BYOD, la doctrine[109] met en exergue le fait que la requête pourrait porter sur le recours à un fournisseur de service *Cloud*, respectivement sur le lieu où les données sont stockées et les conditions de sécurité. Il est douteux pour certains que la réponse à cette question doive comporter autre chose que l'indication du pays dans lequel les données sont conservées et/ou traitées[110]. On ne pourrait par exemple exiger d'avoir accès au contrat avec le sous-traitant ou aux conditions de sécurité.

Savoir où se trouvent les données nous paraît un minima tout comme le fait de pouvoir être assuré que les conditions fixées par la loi pour la communication transfrontière de données (cf. art. 6 LPD) sont respectées. Le secret des affaires s'oppose certes à une divulgation d'informations de nature économique, mais il ne faut pas oublier que, dès que le salarié connaîtra la solution qui a été choisie, il lui sera aisé d'obtenir des informations. Mieux vaut donc jouer la transparence, car tout ce qui est occulté suscite interrogations et doutes.

C. Atteinte illicite à la personnalité de l'employé (328*b* CO)

1. Teneur et portée de l'article 328*b* du CO

Selon l'article 328*b* du 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 ». Il ne peut en aucun cas être dérogé à l'art. 328*b* CO au détriment de l'employé, même si ce dernier y consent (art. 362 al. 1 CO).

Le traitement de données personnelles par l'employeur constitue une source potentielle d'atteinte illicite à la personnalité des travailleurs[111]. L'article 328*b* CO protège l'ensemble de la vie privée et professionnelle du travailleur[112]. Il énumère les deux catégories de données personnelles que l'employeur est autorisé à traiter et rappelle que les dispositions de la LPD s'appliquent également dans les rapports de travail[113]. Les nombreuses informations que détiennent les employeurs sur leurs employés, conjuguées au

109 MÖSSNER, § 2.2.5, p. 33.
110 MÖSSNER, § 2.2.5 avec de nombreuses réf. citées, p. 33.
111 DUNAND, N 1 ad art. 328*b* CO, p. 318.
112 *Ibidem.*
113 *Ibidem*.

développement fulgurant des moyens techniques, en particulier de l'informatique, exposent les travailleurs à des atteintes importantes à leur personnalité[114].

La portée de la disposition est controversée[115]. Jean-Philippe Dunand considère[116] dans ces conditions (en se référant à l'ATF 130 II 425 consid. 3.3) qu'il faut 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* ».

Les deux types de données mentionnées dans la disposition[117] ne présentent pas un intérêt similaire, dans le contexte du BYOD. La première catégorie concerne principalement les dossiers de candidature (le cursus scolaire et professionnel, les diplômes et certificats de travail, les connaissances linguistiques, les autorisations d'exercer [professions réglementées] ou encore les allergies à certaines substances)[118]. La deuxième catégorie affère aux données objectivement et matériellement nécessaires à l'exécution du contrat de travail, c'est-à-dire des données dont l'employeur a besoin pour satisfaire à ses obligations légales ou conventionnelles, ainsi qu'à ses prérogatives d'employeur[119] (état civil, date de naissance, nationalité, numéro AVS, domicile, enfants, références bancaires, relevé des présences et absences, des vacances et heures supplémentaires, fiches de salaire, évaluation des prestations, avertissements, etc.[120]). Font également partie de cette catégorie la correspondance, les contacts professionnels du salarié, les courriels…[121].

Il s'agit pour l'employeur de pouvoir contrôler le respect des devoirs figurant dans le contrat de travail[122]. L'implémentation d'une surveillance tend à s'amplifiquer compte tenu de son coût réduit, de l'efficacité des outils[123], de leur simplicité d'utilisation ainsi que des risques ainsi jugulés. Cette surveillance s'exerce sur les outils informatiques de l'entreprise et donc *a fortiori* en matière de BYOD sur les courriers électroniques, les configurations du dispositif utilisé par l'employé ou les journalisations des accès au système et aux applications[124]. Il existe aujourd'hui des logiciels de gestion qui prennent

114 DUNAND, N 3 ad art. 328*b* CO, p. 319.
115 DUNAND, N 4 ad art. 328*b* CO, p. 319.; MEIER, N 2032 ss, p. 650 ; BALZAN, p. 5 ss.
116 DUNAND, N 4 ad art. 328*b* CO, p. 319.
117 1) Aptitudes de l'employé à remplir son travail ; 2) Données nécessaires à l'exécution du contrat.
118 MEIER, N 2045, p. 654.
119 DUNAND, N 29 ad art. 328*b* CO, p. 326.
120 MEIER, N 2046, p. 654 ; DUNAND, N 29 ad art. 328*b* CO, ainsi que les nombreuses réf. citées, p. 326 et 327.
121 ROSENTHAL, N 37, 39 et 41 ad art. 328*b* CO.
122 ATF 130 II 425, consid. 4.2.
123 Pour un exemple de logiciel de surveillance comportant des fonctionnalités étendues : http://www.netespion.com (consulté le 18 décembre 2013).
124 MÖSSNER, § 2.2.5, p. 35.

en charge le déploiement et le suivi d'une flotte d'appareils mobiles hétérogènes. Il s'agit des *Mobile Device Management*[125]. Ils savent contrôler les appareils à distance et, si besoin, effacent leurs données, surveillent leur activité et veillent au respect des règles de bonne conduite que vous aurez définies vous-même (ne pas utiliser la 3G en roaming, taper un code Pin pour activer l'appareil, etc.)[126]. S'agissant spécifiquement de la surveillance qui peut être opérée, voici les fonctionnalités dont dispose l'une des solutions leader du marché[127], respectivement les informations auxquelles vous pouvez accéder d'un simple clic :

- niveau de charge de la batterie ;
- applications installées ;
- communications passées ;
- position GPS du mobile ;
- possibilité de retracer sur une carte géographique le parcours du téléphone lors des dernières heures ;
- possibilité de prendre une capture de l'écran afin de regarder ce que fait l'utilisateur…

Voici par ailleurs ce qu'indique la plaquette de présentation du produit[128] :

- surveiller à la fois le statut de santé et les statistiques des appareils et du réseau à la recherche d'exceptions ;
- effectuer un suivi de l'activité de l'utilisateur, avec notamment les téléchargements d'applis, la voix, les SMS et l'utilisation de données en violation des seuils prédéfinis, ou encore les listes blanches ou noires ;
- surveiller l'accès au système et l'activité de l'utilisateur sur la console via des fichiers journaux d'événements ;
- établir des alertes et des règles commerciales automatisées pour des actions sur des appareils ou réseaux spécifiques, des actions d'utilisateur ou des performances système ;
- générer des rapports donnant matière à des poursuites avec la distribution automatisée à travers l'équipe de Technologie et information.

---

125 Le *Mobile Device Management* pourra être couplé avec un *Mobile Device Security*.

126 Airwatch, Citrix Xen-mobile et MobileIron gèrent les appareils de toutes les marques et de tous les types et comptent parmi les références du *Mobile Device Management*.

127 Voir DELPRATO.

128 Airwatch, la gestion d'appareils portables et de téléphones intelligents de l'entreprise : https://www.webdepot.umontreal.ca/Usagers/lavoiem/MonDepotPublic/powerpoint/aAirWatch%20Brochure%20-%20Generic%20-%20French.pdf (consulté le 18 décembre 2013).

Activer l'ensemble des options de surveillance contreviendrait, à l'évidence, aux normes applicables en droit suisse[129]. En matière de BYOD, les trois principales solutions du marché proposent toutes des outils de surveillance, lesquels sont devenus un standard. Il y a donc automatiquement surveillance.

Le salarié doit donner son accord formel avant l'installation d'un « *Mobile device managment* ». Comme il a été exposé précédemment, ce consentement doit être éclairé, c'est-à-dire délivré après une orientation exhaustive des fonctionnalités du « *Mobile device managment* » (modalités de contrôle, de filtrage et de suspension de la partie dédiée aux usages professionnels…) et des buts poursuivis notamment. Cet accord devra être formalisé de préférence dans la charte BYOD.

En cas de surveillance des salariés, celle-ci devra se conformer à l'article 328*b* du CO[130]. Une autre disposition trouvera application, l'article 26 de l'Ordonnance 3 relative à la loi sur le travail (Hygiène, OLT 3) du 18 août 1993[131], dont la teneur est la suivante : « *Il est interdit d'utiliser des systèmes de surveillance ou de contrôle destinés à surveiller le comportement des travailleurs à leur poste de travail. Lorsque des systèmes de surveillance ou de contrôle 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* »[132]. Cette disposition constitue une référence permettant de tracer la ligne rouge en matière de surveillance entre le contrôle objectif de l'activité professionnelle et la surveillance comportementale proscrite. L'employé devra quant à lui être exhaustivement informé de la nature, de l'ampleur et du but de la surveillance[133].

Henrique Mössner a accompli un excellent travail de comparaison entre la situation ordinaire de traitement des données nécessaire à l'exécution du contrat de travail et une situation où le BYOD a été implémenté[134]. Il en résulte que si le scan des courriels n'engendre pas de risque supplémentaire[135], il en va différemment en ce qui concerne les données personnelles et professionnelles. Soit celles-ci sont sauvegardées séparément sur le dispositif privé, soit elles sont mélangées, cette dernière hypothèse engendrant bien évidemment un risque accru d'atteintes aux droits des salariés. L'effacement des données

129 A titre exemplatif, la surveillance en temps réel de la position GPS du mobile est illicite (ATF 130 II 425).

130 L'article 4 al. 2 LPD qui comprend les principes généraux est également applicable en vertu du renvoi de l'article 328*b* al. 2 CO.

131 RS 822.113.

132 Alinéa 2.

133 BIRKHÄUSER/HADORN, p. 165.

134 MÖSSNER, § 2.3.2, p. 36 ss.

135 Même s'il y a potentiellement plus de courriels privés, car la surveillance demeure anonyme.

suscite également des problématiques spécifiques, notamment si les données sont mergées. Le risque majeur mis en exergue a trait à la destruction des données privées. De ce point de vue, il paraît essentiel de faire figurer dans la charte BYOD une disposition qui oblige le salarié à effectuer des sauvegardes régulières de ses données privées (cf. *infra* IV.A). Il paraît également opportun de réglementer précisément la procédure d'effacement à distance.

2. Sanctions de la violation de l'article 328*b* du CO

L'article 15 LPD prévoit que le lésé agisse en justice sur le plan civil (art. 28, 28*a* et 28l CC) pour requérir l'interdiction du traitement de données (notamment la communication à des tiers), leur rectification ou leur destruction. L'article 15 al. 2 LPD prévoit en sus des actions civiles précitées, la possibilité de faire mentionner le caractère litigieux à la donnée. En matière de protection des données, d'autres dispositions pourraient trouver application comme le droit d'accès (art. 8 LPD[136]), le droit de solliciter la rectification (art 5 al. 2 LPD), le blocage ou l'effacement des données (art. 15 al. 1 LPD). Le salarié dispose également de la possibilité de saisir la justice sur la base des clauses de son contrat de travail. Il y a concours entre ces deux moyens[137].

Les actions fondées sur l'article 15 LPD, respectivement les articles 28, 28*a* et 28l CC seront rares. Henrike Mössner évoque[138] l'hypothèse d'une action en cessation de l'atteinte à la personnalité, lorsque la personne concernée apprend que les données la concernant sont, par exemple, transférées à l'étranger (cf. III.A.3). Or, d'ordinaire, l'employeur ne communique pas sur de tels faits, même s'il pourrait être légalement obligé de le faire (cf. III.A.2). Le salarié devra donc l'apprendre de tiers.

Le salarié pourra agir en dommages et intérêts sur la base des normes contractuelles[139]. Comme le salarié doit apporter la preuve tant du dommage que celle de la faute, il est à craindre que cette voie ne soit semée d'embûches. Citons par exemple la révélation des préférences sexuelles d'un salarié, laquelle n'est pas en adéquation avec l'activité professionnelle déployée par l'entreprise et qui *de facto* entraîne une impossibilité de poursuivre la collaboration.

De surcroît, l'auteur du traitement de données sera tenté d'exciper de l'existence de l'un des faits justificatifs de l'article 13 al. 1 LPD, soit le consentement, la loi et l'intérêt

---

136 Avec la possibilité d'agir en exécution (art. 15 al. 4 LPD) selon la procédure simplifiée du Code de procédure civile du 19 décembre 2008 et celle de déposer une plainte pénale (art. 34 LPD) en cas de violation intentionnelle du droit d'accès.

137 MEIER, N 1728, p. 566.

138 MÖSSNER, § 3.1, p. 39.

139 Cf. MEIER, N 1783, p. 580 et les nombreux exemples cités.

prépondérant. L'employeur pourrait invoquer l'existence d'un intérêt privé prépondérant économique. Il devra apporter la preuve de l'existence, de la nature et de la portée de cet intérêt. S'agissant du consentement, par nature libre et éclairé, il devra porter sur toutes les opérations qui peuvent techniquement être diligentées sur l'appareil privé et sur tous les traitements de données, lesquels devront être précisément listés et décrits. Ces informations qui permettront, en cas de litige, d'apporter la preuve de l'accord du salarié devront figurer dans la charte BYOD.

Le risque de porter atteinte aux intérêts du salarié ne se concrétisera que dans de rares hypothèses. La transparence et le contrat de confiance (charte BYOD) sont des éléments qui doivent réduire ce risque, le juguler. Il existe une corrélation entre les mesures techniques et la réglementation qui doit conduire à ce que les atteintes soient les plus minimes possible et si, extraordinairement elles devaient survenir, être réglées par voie amiable par exemple en prévoyant un arbitrage entre employeur et employé. La saisine des tribunaux aurait en effet pour conséquence d'anéantir la confiance dans le processus BYOD.

IV. Règles applicables en matière de droit pénal

A. Détérioration de données (art. 144bis CP)

La question principale a trait à la protection des données personnelles du salarié. L'employeur peut en effet techniquement procéder à un effacement de toutes les informations, respectivement données contenues dans l'appareil d'un employé à distance (on parle de *Device Wiping*), notamment en cas de perte ou de vol. Ainsi, l'article 144bis du Code pénal (détérioration de données[140]) qui protège l'intégrité des données pourrait-il trouver application. L'effacement des données professionnelles ne génère pas de difficulté. Il en va différemment des données personnelles. Si les données sont séparées, par exemple par le biais de la création d'un espace professionnel dédié dans l'appareil personnel du salarié, l'effacement à distance pourra s'opérer dans le respect des droits de ce

[140] *Celui qui, sans droit, aura modifié, effacé, ou mis hors d'usage des données enregistrées ou transmises électroniquement ou selon un mode similaire sera, sur plainte, puni d'une peine privative de liberté de trois ans au plus ou d'une peine pécuniaire.*
Si l'auteur a causé un dommage considérable, le juge pourra prononcer une peine privative de liberté de un à cinq ans. La poursuite aura lieu d'office.

dernier. Si les données sont fusionnées, tout effacement est problématique, sous peine de violer l'article 144bis CP précité[141].

Il s'agit d'une infraction qui se poursuit sur plainte, sauf en cas de dommage considérable[142], ce qui pourrait être le cas si la récupération et/ou la reconstitution des données effacées nécessite beaucoup de temps ou le recours à un informaticien par exemple, ou si elles ont une valeur marchande (bibliothèque musicale). Cette notion devant être interprétée tant au regard de limites concrètes que d'éléments subjectifs, l'effacement de photographies d'enfants ou de moments heureux vécus en famille pourrait réaliser la condition légale. Il a en effet été jugé[143] que les déprédations occasionnées dans un appartement par des cambrioleurs pour CHF 10'000.- représentent un montant objectivement important, cela d'autant plus que les dommages causés constituent pour la victime une atteinte d'une valeur affective difficilement estimable. Par analogie et dans l'hypothèse où le dommage objectif atteindrait cette somme, il pourrait être considéré que les données personnelles figurant sur l'appareil privé (photos, messages, vidéos, musique, etc.) ont une valeur affective notable, générant ainsi une poursuite d'office. Il est en effet fréquent, actuellement, que le *device* constitue simultanément à l'outil de travail dématérialisé, l'appareil photo, le caméscope ou encore le juke-box numérique de la famille.

Il est donc conseillé d'intégrer une clause dans la charte BYOD qui prévoit que l'employé devra effectuer des sauvegardes régulières de ses données personnelles. L'employeur ne diligentera quant à lui qu'une sauvegarde des données professionnelles. En cas de violation de cette obligation par l'employé, cela n'exonérera pas l'employeur de devoir expliquer l'effacement des données personnelles[144], mais pourrait entrer en ligne de compte dans le cadre de l'application des articles 52 (absence d'intérêt à punir) et 53 CP (réparation) relatifs aux motifs pour l'exemption de peine[145]. Sur le plan civil, une telle clause influera par contre assurément sur l'issue d'un éventuel litige, dans la mesure où une faute concomitante pourra être retenue à la charge de l'employé qui réclamerait la réparation du dommage.

---

141 BIRKHÄUSER/HADORN, p. 201.

142 Par analogie avec la notion de dommage considérable de l'article 144 CP, cf. RSJB 121, p. 511.

143 RSJB 121, p. 151.

144 Qui pourrait, entre autres, intervenir par accident.

145 Par renvoi des articles 8 et 319 al. 1 let. e du Code de procédure pénale du 5 octobre 2007 (RS 312.0).

B. Violation de secrets privés (art. 179 CP)

Il existe également un risque de prise de connaissance de courriels privés. Dans une telle hypothèse, une violation de l'article 179 CP (violation de secrets privés) dont la teneur est la suivante pourrait survenir : « *Celui qui, sans en avoir le droit, aura ouvert un pli ou colis fermé pour prendre connaissance de son contenu, celui qui, ayant pris connaissance de certains faits en ouvrant un pli ou colis fermé qui ne lui était pas destiné, aura divulgué ces faits ou en aura tiré profit, sera, sur plainte, puni d'une amende* ». L'e-mail est protégé par cet article[146], à tout le moins lorsque celui-ci est « fermé », notamment par un mot de passe, respectivement lorsque l'expéditeur manifeste clairement qu'un tiers ne peut sans autre prendre connaissance du message[147]. La prudence s'imposera donc si les courriels de l'entreprise sont réceptionnés par exemple dans le même logiciel de messagerie[148].

Une telle manifestation du caractère privé peut intervenir par le biais d'une mention explicite signalant qu'il s'agit d'un envoi privé par exemple dans le champ « objet » du courriel (personnel/privé ou c/o)[149]. Le champ peut également mentionner un objet qui, sans équivoque, relève du domaine privé[150].

En cas de doute sur la nature d'un message, il convient de ne pas le lire, mais de rendre le destinataire attentif au problème et lui demander si le courriel en question est de nature privée ou non. Relativement à la problématique de la surveillance des courriels, il semble opportun de préciser que celle-ci ne saurait porter systématiquement sur les messages de

---

146 En France, la Cour de cassation, dans un arrêt fondateur, Cass. soc., 02-10-2001, n° 99-42942 dit arrêt « Nikon », disponible à cette adresse : http://www.courdecassation.fr/jurisprudence_2/chambre_sociale_576/arret_n_1159.html (consulté le 18 décembre 2013) a posé le principe que le salarié a droit, même au temps et au lieu de travail, au respect de l'intimité de sa vie privée et que celle-ci implique en particulier le secret des correspondances : l'employeur ne peut, sans violation de cette liberté fondamentale, prendre connaissance des messages personnels émis par le salarié et reçus par lui grâce à un outil informatique mis à sa disposition pour son travail et ceci même au cas où l'employeur aurait interdit une utilisation non professionnelle de l'ordinateur.

147 MONNIER, p. 141 ss ; VON INS/WYDER, N 18 ss ad art. 179 ; TRECHSEL/LIEBER, N 5 ad art. 179 ; HURTADO POZO, §80 N 2176.

148 A terme, il devrait être possible de splitter dans des logiciels différents les messages par nature essentiellement professionnels et ceux essentiellement personnels.

149 Le fait que le nom de la personne figure avant le nom de l'entreprise, sur une lettre, ne suffit pas pour déterminer que l'envoi est de nature privée, selon le Préposé fédéral à la protection des données et à la transparence : http://www.edoeb.admin.ch/datenschutz/00763/00807/00827/index.html ?lang=fr (consulté le 18 décembre 2013).

150 Cf. MEIER, N 2183, p. 705, qui cite comme exemples : « notre sortie du week-end prochain » ; « cadeau de mariage de X ».

nature non professionnelle ou non signalés comme privés, sans justification objective, annonce préalable et respect du principe fondamental de la proportionnalité.

Il convient donc de préciser que pour que les documents, e-mails, fichiers et autres aient un caractère privé opposable à l'employeur, il incombe au salarié de les identifier comme privés, aussi bien pour les éléments stockés que les courriers électroniques entrant ou sortant. Lorsque le fichier ou le message ne comporte pas de champ « objet » comme cela peut être le cas pour un SMS ou un message instantané[151], il faut impérativement que le lecteur puisse identifier le texte comme « privé » à sa première lecture. La jurisprudence est relativement rare s'agissant des dossiers électroniques ou des répertoires[152]. En France, il a été jugé que ne sont pas couvert par le droit à la vie privée :

- un dossier identifié par les seules initiales du salarié (Cass. soc. 21-10-2009, n° 07-43.877[153]) ;
- un répertoire désigné par le prénom du salarié (Cass. soc. 21-10-2009, n° 0743.877) ;
- les fichiers accessibles sous la dénomination « mes documents » (Cass. soc. 10-5-2012, n° 11-13884[154]) ;
- les documents classés dans un dossier intitulé « données personnelles » si l'utilisateur ne les a pas identifiés individuellement comme privés (Cass. soc. 04-07-2012, n° 11-22972).

Ces différentes règles, difficiles à appréhender pour le néophyte, doivent figurer explicitement dans la charte à soumettre au salarié (cf. VI). Le principe de transparence qui est l'un des piliers du BYOD l'impose. L'employeur aura par ailleurs tout intérêt à délivrer toutes les informations juridiques pour éviter que ses salariés n'excipent d'un consentement non éclairé à l'introduction du BYOD si un problème devait survenir.

151 A l'instar de WhatsApp ou de la messagerie de Facebook.

152 Pour de plus amples informations, cf. Guide pour le traitement des données personnelles dans le secteur du travail, Traitement par des personnes privées, Mai 2001, disponible à cette adresse : http://www.edoeb.admin.ch/datenschutz/00763/index.html ?lang=fr (consulté le 18 décembre 2013).

153 Accessible à cette adresse : http://www.legifrance.gouv.fr/affichJuriJudi.do ?idTexte=JURITEXT000021194925 (consulté le 18 décembre 2013).

154 Accessible à cette adresse : http://www.legifrance.gouv.fr/affichJuriJudi.do ?idTexte=JURITEXT000025861623 (consulté le 18 décembre 2013).

V. Règles applicables en matière de propriété intellectuelle

A. Exception d'usage privé (art. 19 LDA)

Le collaborateur est à l'évidence responsable du respect des droits de propriété intellectuelle des éléments non professionnels se trouvant dans son matériel. Il convient toutefois de le lui rappeler expressément dans le cadre de la charte BYOD (cf. VI), par exemple en ces termes : *Les utilisateurs sont pleinement et exclusivement responsables de tous les éléments non professionnels figurant dans leur matériel (logiciels, éléments de propriété intellectuelle, images, etc.). Le transfert des éléments soumis à des droits de propriété intellectuelle est formellement interdit, sans l'accord explicite préalable de l'employeur. Les utilisateurs sont rendus attentifs au fait que l'induction dans le système d'information de l'entreprise, en violation de ce devoir, peut engendrer une action récursoire de l'employeur, si celui-ci doit en subir un dommage et en toutes hypothèses une sanction pouvant conduire jusqu'à un licenciement immédiat.*

Nous ne nous interrogeons pas naturellement sur la nécessité d'acquérir des licences ou des droits de propriété intellectuelle du fait de l'installation d'applications « métier » sur les appareils privés des salariés et *a fortiori* de leur utilisation. Chacun aura tendance à considérer que la licence permet une telle utilisation, invoquant implicitement un droit à la copie privée[155], soit une utilisation de l'œuvre à des fins privées (article 19 de la Loi fédérale sur le droit d'auteur et les droits voisins du 9 octobre 1992)[156]. L'exception d'usage privé au sens étroit n'est pas un droit à la copie privée, mais une restriction au droit d'auteur[157]. Au sens large, il s'entend comme un usage non commercial.

Or, selon l'article 19 al. 4 LDA l'exception d'usage privé ne saurait s'appliquer aux logiciels au motif que *l'auteur aurait des difficultés à assurer l'exploitation commerciale de son œuvre*[158]. La copie d'un logiciel même partielle, même provisoire, n'est autorisée ni pour l'usage strictement personnel, ni pour les besoins de l'enseignement scolaire, ni à l'intérieur des entreprises ou des administrations publiques[159]. Conséquemment, seules sont autorisées les copies durables ou passagères qui sont réalisées dans le cadre de l'utilisation autorisée[160] et les copies de sauvegarde. Dans ces conditions, il n'est pas

155 BERANEK ZANON, N 17 à 29.
156 (LDA), RS 231.1.
157 DESSEMONTET, N 142, p. 102.
158 BARRELET/EGLOFF, N 29, p. 131.
159 BARRELET/EGLOFF, N 29, p. 131.
160 Cf. 17 al. 1er let. a ODAu.

possible de soutenir de manière objective une quelconque exception d'usage privé dans le cadre du BYOD.

Il en résulte la nécessité de vérifier le contenu des contrats de licence et en cas de doute de contacter le détenteur des droits pour éclaircir la situation juridique (nombre de licences, type, sous-licence autorisée, etc.). La gestion des licences est donc stratégique[161]. A défaut, l'entreprise pourrait devoir répondre d'une violation tant sur le plan civil que pénal. Le salarié devra également être rendu attentif à la nécessité de ne pas autoriser des tierces personnes à se servir de son *device* pour réaliser une activité qui s'apparenterait à une activité commerciale. L'accès à ces logiciels devra finalement être sécurisé pour éviter toute utilisation indue (verrouillage par mot de passe, etc.).

B. Droit sur des inventions et des designs (art. 17 LDA et art. 332 CO)

Se pose également la question de savoir à qui appartiennent les résultats de l'activité professionnelle accomplie au moyen de l'appareil personnel. La loi est, à cet égard, très claire. L'article 332 alinéa 1er du CO postule que les inventions que le travailleur a faites et les design qu'il a créés, ou à l'élaboration desquels il a pris part, dans l'exercice de son activité au service de l'employeur et conformément à ses obligations contractuelles, appartiennent à l'employeur, qu'ils puissent être protégés ou non. L'article 17 LDA (intitulé « droits sur les logiciels » prévoit que l'employeur est seul autorisé à exercer les droits exclusifs d'utilisation sur le logiciel créé par le travailleur dans l'exercice de son activité au service de l'employeur et conformément à ses obligations professionnelles. Le fait que le logiciel ait été créé sur le lieu de travail ou ailleurs, pendant les heures de travail ou en dehors ne joue aucun rôle[162]. L'élément déterminant est que la création intervienne en exécution des obligations contractuelles[163].

Peu importe donc du point de vue légal au moyen de quel appareil les résultats de l'activité professionnelle ont été obtenus. Les négociations avec le salarié d'un droit sur les inventions réalisées en dehors de l'accomplissement des obligations contractuelles vont s'intensifier dans ce cadre et du fait de manière plus générale de la dématérialisation de l'activité professionnelle (art. 332 al. 2 CO).

---

161 BERANEK ZANON, N 39 à 41.
162 ATF du 9 novembre 1983, RSPI 1984. p. 262 s.
163 In : sic ! 1997, p. 382.

VI. Charte BYOD (BYOD Policy)

Ainsi que cela a été évoqué lors des différentes étapes de l'analyse des risques juridiques, une charte est absolument nécessaire pour formaliser les droits et les devoirs de chaque partie. Une telle charte devrait être paraphée par chaque employé pour éviter des contestations ultérieures, respectivement pour qu'il puisse être constaté que le consentement recueilli était éclairé. En pratique, nous procédons en plusieurs étapes. Après avoir étudié l'opportunité technique et stratégique de l'implémentation du BYOD, il s'agit d'expliciter les impacts juridiques et sociaux de la mise en œuvre au sein de l'entreprise. Associer les instances représentatives du personnel de l'entreprise est important, déjà à ce stade. Finalement la charte doit apparaître comme le garant d'une exploitation conforme aux normes et aux intérêts de chacun. La transparence est une condition absolue de réussite d'un tel processus complexe. L'employeur doit, de ce point de vue, prendre le temps d'expliciter les solutions techniques, leur impact pour chacun et les choix qui ont été opérés non seulement sur le plan juridique, mais également stratégique. La charte devra certainement faire l'objet de mises à jour régulières, ce qui peut générer des difficultés s'agissant de la nécessité déjà exposée qu'elle soit paraphée par les salariés. Une des solutions pour éviter cet écueil consisterait à la rédiger en des termes technologiquement neutres pour qu'elle soit évolutive à tout le moins s'agissant des appareils (cf. Google Glass) et des logiciels de BYOD. Les normes juridiques pourraient quant à elles être exposées et explicitées par le biais d'exemples en réservant les décisions qui seraient rendues à l'avenir. La qualité de rédaction d'une telle charte devrait épargner bien des tracas aux entreprises qui souhaitent opter pour le BYOD.

VII. Conclusions

Le BYOD n'en est qu'à ses balbutiements juridiques. Sur le plan technique, tous les outils nécessaires à son développement sont accessibles et implémentables rapidement et relativement facilement. Preuve en est le taux d'adoption considérable mis en exergue dans nos entreprises. Cette discrépance doit engendrer chez l'employeur une réflexion rapide aux fins d'éviter d'avoir à régler ou à apprendre lors de procédures que les choix opérés n'étaient pas en conformité avec la loi. Dans un tel cas, le risque hormis légal sera de porter atteinte à la réputation de l'entreprise qui aura alors naturellement tendance à accroître la compliance, ce qui anéantirait les efforts consentis par l'employeur et l'employé pour augmenter la productivité et la satisfaction mutuelle. Une telle démarche accomplie dans la confiance et en toute transparence des normes à respecter *ab initio* responsabilisera au contraire chacun. Il en résultera assurément une facilité d'adaptation aux nouveaux standards juridiques qui ne manqueront pas de s'imposer dans les pro-

chaines années. Introduire le BYOD en respectant les règles est une nécessité, mais maintenir la matrice normative à jour s'avérera une tâche plus contraignante dont on ne saurait s'exonérer. Il s'agit donc d'une démarche de longue haleine qui, après une phase initiale qui prendra d'ordinaire plusieurs mois, se poursuivra chaque année lorsqu'il s'agira de procéder aux contrôles périodiques du respect de la légalité des processus. Tout ceci bien évidemment pour éviter que le BYOD ne devienne pour l'entreprise et le salarié un Bring Your Own Disaster !

VIII. Bibliographie

ANDY JACQUES, Le BYOD : première étape d'une stratégie de productivité mobile, in : Journal du Net, 25 avril 2013 : http://www.journaldunet.com/ebusiness/expert/54047/le-byod---premiere-etape-d-une-strategie-de-productivite-mobile.shtml (consulté le 18 décembre 2013).

ARNING/MOOS/BECKER, Vertragliche Absicherung von Bring Your Own Device – Was ist einer Nutzungvereinbarung zu BYOD mindestens enthalten sein sollte, Computer und Recht 09/2012, p. 592-598 (www.computerundrecht.de).

BALZAN MARIE-CHRISTINE, La protection des données des travailleurs dans la due diligence, in : WYLER (édit.), Panorama II en droit du travail, Berne 2012.

BARRELET/EGLOFF, Le nouveau droit d'auteur, Commentaire de la Loi fédérale sur le droit d'auteur et les droits voisins, 3e éd., Berne 2008.

BERANEK ZANON NICOLE, Bring your own device (BYOD) aus rechtlicher Sicht, Jusletter IT 12 septembre 2012.

BIRKHÄUSER/HADORN, BYOD – Bring Your Own Device, Schweizerische Juristen-Zeitung 109/2013, p. 201 ss.

CAUVIN EMMANUEL, Obligation de connexion, liberté de déplacement : le contrat de travail réinvité, article publié sur le site Les Echos.fr : http://lecercle.lesechos.fr/economie-societe/social/relations-sociales/221180728/obligation-connexion-liberte-deplacement-contra (consulté le 18 décembre 2013).

CHABOT FLAVIO-GABRIEL, La protection des données à la lumière de deux exemples tirés de l'actualité récente, Bulletin CEDIDAC n° 57, octobre 2011.

CROCHET-DAMAIS ANTOINE, BYOD : indemniser les salariés… ou pas ?, in : http://www.journaldunet.com/solutions/mobilite/bring-your-own-device-byod-dans-les-dsi/byod-deux-grandes-politiques.shtml (consulté le 18 décembre 2013).

DELPRATO JEAN-MARC, Gérez facilement vos mobiles d'entreprise avec Airwatch, 5 septembre 2013 : http://www.01net.com/editorial/603264/gerez-facilement-vos-mobiles-dentreprise-avec-air watch/ (consulté le 18 décembre 2013).

DESSEMONTET FRANÇOIS, La propriété intellectuelle et les contrats de licence, Lausanne 2011.

DUNAND JEAN-PHILIPPE, in : DUNAND/MAHON, Commentaire du contrat de travail, Berne 2013.

EBNETER MATHIAS, Informationspflichten im Zusammenhang mit « Data Security Breaches », Jusletter 7 juin 2010.

EYNARD JESSICA, Les données personnelles, Quelle définition pour un régime de protection efficace ?, Paris 2013.

FANTI SÉBASTIEN, Cloud computing : opportunités et risques pour les avocats, Revue de l'avocat 2/2013, p. 74-77.

FLUCKIGER ALEXANDRE, L'autodétermination en matière de données personnelles : un droit (plus si) fondamental à l'ère digitale ou un nouveau droit de propriété ?, PJA 2013, p. 837 ss.

HURTADO POZO JOSÉ, Droit pénal, Partie spéciale, Zurich 2009.

LEBLAL SERGE, Avec Knox, Samsung renforce la sécurité d'Androïd dans les entreprises, in : Le Monde informatique, 23 septembre 2013 : http://www.lemondeinformatique.fr/actualites/lire-avec-knox-samsung-renforce-la-securite-d-android-dans-les-entreprises-55117.html (consulté le 18 décembre 2013).

LELIÈVRE HÉLÈNE, Le BYOD, une réalité dans 9 entreprises suisses sur 10, in : ICT journal du 8 novembre 2012 : http://www.ictjournal.ch/fr-CH/News/2012/11/08/Le-BYOD-une-realite-dans-9-entreprises-suisses-sur-10.aspx (consulté le 18 décembre 2013).

LETSCH THOMAS, Rechtliche Aspekte von Work-Life-Balance, Berne 2008.

LEWIS PETER H., Forget Big Brother, New York Times, 19 mars 1998.

MANARA CÉDRIC, Réseaux sociaux : 101 questions juridiques, Paris 2013.

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

MONNIER GILLES, Le piratage informatique en droit pénal, sic ! 2009, p. 141 ss.

MORIN JEAN-HENRY, L'utilisation des moyens techniques en vue d'une amélioration de la protection des données, in : Le développement du droit européen en matière de protection des données et ses implications pour la Suisse, Bâle 2012.

MÖSSNER HENRIKE, Bring your own device (BYOD) : Quelle problématique se pose pour l'employeur sous l'angle de la protection des données ?, Mémoire présenté en vue de l'obtention de la Maîtrise universitaire en droit, criminalité et sécurité des technologies de l'information, Janvier/Février 2013.

MÜLLER ROLAND A., OFK-MÜLLER, Kommentar ArG 17*b* Abs. 1, Zurich 2009.

NESTENREKO MICHEL, Bull plus fort que la NSA : peut-on croire aux smartphones sécurisés ?, 4 octobre 2013, http://www.atlantico.fr/decryptage/bull-plus-fort-que-nsa-peut-on-croire-aux-smart phones-securises-michel-nesterenko-860583.html (consulté le 18 décembre 2013).

RAY JEAN-EMMANUEL, Le BYOD et le droit du travail, 16 novembre 2012 : http://www.lecafedudroit.fr/le-byod-bring-your-own-device-apportez-votre-propre-materiel-et-le-droit-du-travail/ (consulté le 18 décembre 2013).

REUTTER/KLAUS, Rechtliche Stolpersteine bei « BYOD », Digma 2012, p. 160 ss.

ROSENTHAL DAVID, Handkommentar DSG, Zurich 2008.

SECRÉTARIAT D'ÉTAT À L'ÉCONOMIE (SECO), Commentaire de la loi sur le travail article par article, http://www.seco.admin.ch/themen/ 00385/00390/00392/02064/index.html?lang=fr (consulté le 18 décembre 2013).

STAUDER BERND, in : THEVENOZ/WERRO (édit.), Commentaire romand, Code des obligations, Bâle 2012.

TRECHSEL STEFAN, Schweizerische Strafgesetzbuch, Praxiskommentar, Zurich 2008.

VON INS/WYDER, Basler Kommentar, Strafgesetzbuch II, Bâle 2003.

WALTER JEAN-PHILIPE, Communication de données à l'étranger, in : EPINEY/HOBI (édit.), La révision de la Loi sur la protection des données, Zurich 2009.

WHITAKER REG, Big Brother.com., La vie privée sous surveillance, Les Presses de l'Université Laval 2001.

GENEVIÈVE ORDOLLI

Utilisation d'Internet et de l'intranet par les syndicats et les représentants élus des travailleurs

Sommaire

I. Introduction 206

II. Bases légales 207
A. Représentants élus 207
1. Champ d'application 208
2. Condition 209
B. Syndicats 211
1. Salariés syndiqués 211
2. Syndicalistes non employés dans l'entreprise 212

III. Questions particulières 213
A. Affichage sur l'intranet 213
1. Représentants élus 213
a) Conditions 213
aa) Equipement informatique de l'entreprise 213
bb) Usage de l'intranet dans l'entreprise 213
cc) Proportion de travailleurs ayant accès à l'intranet dans l'entreprise 213
dd) Secteur d'activités et taille de l'entreprise 214
ee) Configuration de l'entreprise 214
b) Modalités 214
aa) Coûts 214
bb) Etendue de l'affichage 214
cc) Contenu 215
2. Syndicats 216
B. Messagerie électronique dans l'entreprise 218
1. Représentants élus 218
a) Conditions 218
b) Modalités 218
aa) Contenu 218
bb) Envoi en masse 219
cc) Liste d'adresses 219
2. Salariés syndiqués 220
a) Absence de réglementation 220
b) Directive ou convention collective 221

C. Messagerie électronique de et vers l'entreprise 222
1. Représentants élus 222
2. Syndicats 222

IV. Conclusion 224

Bibliographie 225

I. Introduction

Envoi de tracts syndicaux par courriel, affichage d'informations par la représentation des travailleurs sur l'intranet de l'entreprise… et si la communication entre les salariés et leurs représentants passait aussi par Internet et par l'intranet de l'entreprise ? L'utilisation d'Internet et de l'intranet dans l'entreprise par les représentants des travailleurs, élus ou syndicaux, se heurte au but visé par l'employeur lorsqu'il met en place l'accès à ces réseaux dans l'entreprise. L'étendue de cette utilisation dépend donc d'un arbitrage entre l'intérêt de l'employeur à ce que ces réseaux soient utilisés uniquement à des fins économiques, et celui des représentants des travailleurs à informer et communiquer avec les travailleurs également par le biais de ces réseaux.

Le système suisse de représentation collective des travailleurs est dualiste : il comprend d'une part les représentants élus par les travailleurs au sein d'une entreprise ou partie d'entreprise[1], d'autre part les associations professionnelles communément nommées syndicats.

De même, l'intranet désigne un réseau électronique interne à l'entreprise, alors qu'Internet relie l'entreprise au monde extérieur. Ces technologies apportent des avantages indéniables en termes de rapidité, de commodité voire de discrétion (la communication entre les travailleurs et leurs représentants par l'intermédiaire de ces réseaux n'est en principe pas visible par la clientèle). Revers de la médaille, le risque d'une utilisation abusive de ces moyens est démultiplié en raison des caractéristiques précédemment évoquées.

Après une présentation des bases légales applicables, nous examinerons trois questions : (A) le droit des représentants des travailleurs d'afficher des informations sur l'intranet de l'entreprise ; (B) l'utilisation de la messagerie électronique professionnelle par les repré-

[1] Voir art. 3 et 4 Loi fédérale sur l'information et la consultation des travailleurs dans les entreprises du 17 décembre 1993 (Loi sur la participation), RS 822.14.

sentants des travailleurs, à l'intérieur de l'entreprise ; (C) l'utilisation de la messagerie électronique par les représentants des travailleurs, de et vers l'entreprise.

II. Bases légales

Alors que l'Allemagne a légiféré en 2001 sur l'utilisation des nouvelles technologies de l'information et de la communication par les comités d'entreprise[2] et que la France a introduit en 2004 des dispositions relatives à l'information syndicale sur l'intranet ou la messagerie électronique de l'entreprise[3], le législateur suisse n'est pas intervenu sur ces questions.

En droit suisse, il s'impose donc d'examiner les questions relatives à l'utilisation d'Internet et de l'intranet par les représentants des travailleurs à la lumière de bases légales non destinées spécifiquement à les régler. En particulier, il convient de se référer d'une part à la Loi fédérale sur la participation, entrée en vigueur en 1994, d'autre part à la liberté syndicale et son application dans les rapports de droit privé.

A. Représentants élus

L'article 11 al. 2 Loi sur la participation prévoit que « l'employeur doit soutenir la représentation des travailleurs dans l'exercice de ses activités. Il met à sa disposition les locaux, les moyens matériels et les services administratifs nécessaires ».

Cette disposition n'a jusqu'ici donné lieu à aucune interprétation par les tribunaux[4].

---

2 § 40 al. 2 Betriebsverfassungsgesetz du 15 janvier 1972 (BetrVG) : « Für die Sitzungen, die Sprechstunden und die laufende Geschäftsführung hat der Arbeitgeber in erforderlichem Umfang Räume, sachliche Mittel, Informations- und Kommunikationstechnik sowie Büropersonel zur Verfügung zu stellen ».

3 Art. L. 2142-6 (= anc. L. 412-8 al. 7) Code du travail du 2 janvier 1973 (CT) : « Un accord d'entreprise peut autoriser la mise à disposition des publications et tracts de nature syndicale, soit sur un site syndical mis en place sur l'intranet de l'entreprise, soit par diffusion sur la messagerie électronique de l'entreprise. Dans ce dernier cas, cette diffusion doit être compatible avec les exigences de bon fonctionnement du réseau informatique de l'entreprise et ne pas entraver l'accomplissement du travail. L'accord d'entreprise définit les modalités de cette mise à disposition ou de ce mode de diffusion, en précisant notamment les conditions d'accès des organisations syndicales et les règles techniques visant à préserver la liberté de choix des salariés d'accepter ou de refuser un message ».

4 La jurisprudence a seulement traité de la collaboration de bonne foi entre employeur et représentation élue (art. 11 al. 1), de laquelle découle une obligation de l'employeur d'examiner avec sérieux les propositions de la représentation des travailleurs dans le cadre de la procédure de consultation rela-

1. Champ d'application

L'article 11 al. 2 ne mentionne pas les moyens électroniques ou virtuels tels qu'Internet ou l'intranet. Entrent-ils néanmoins dans son champ d'application ?

La formulation de l'article 11 al. 2 Loi sur la participation ressemble à celle de la disposition allemande en vigueur avant 2001[5]. Bien que mentionnant uniquement les locaux, le matériel et le personnel de bureau, cette disposition a été appliquée à l'intranet[6]. En droit suisse, la question se pose du choix entre une interprétation large ou, au contraire, restrictive de l'article 11 al. 2 2e phrase Loi sur la participation.

La version italienne de la loi sur la participation utilise des termes équivalents à ceux de la version française : *mezzi materiali*. Le caractère matériel des moyens y est donc également affirmé. Cette exigence n'apparaît en revanche pas dans la version allemande qui parle simplement de moyens (auxiliaires) : *Hilfsmittel*.

Si l'on s'en tient aux versions française et italienne, l'interprétation littérale ne suffit pas pour justifier l'application de ce texte à Internet ou à l'intranet. D'une part, ces réseaux ne constituent pas un moyen matériel, mais un mode d'information et de communication électronique, virtuel et « dématérialisé »[7]. D'autre part, Internet et l'intranet ne sont pas non plus un service administratif tel que la dactylographie d'un procès-verbal de commission du personnel par un secrétaire de l'entreprise ou la diffusion, par un employé, de ce texte aux travailleurs[8] – travaux qui supposent l'intervention du personnel administratif de l'entreprise.

En revanche, l'utilisation d'Internet et de l'intranet par les représentants élus du personnel entre dans le champ d'application de la loi tel que formulé en allemand.

L'absence de concordance entre les différentes versions linguistiques nous oblige à recourir à d'autres « points d'appui »[9] de l'interprétation que le texte même de la loi.

---

tive à un licenciement collectif (voir par exemple ATF 137 III 162, consid. 1.1, JdT 2012 II 202 (rés.).

5 « Für die Sitzungen, die Sprechstunden und die laufende Geschäftsführung hat der Arbeitgeber in erforderlichem Umfang Räume, sachliche Mittel sowie Büropersonal zur Verfügung zu stellen ».

6 Arbeitsgericht Paderborn, 29 janvier 1998, 1 BV 35/97, Arbeit und Recht 1998, p. 342, http://www.online-recht.de (consulté le 10 décembre 2013) : le comité d'entreprise a obtenu le droit d'afficher des informations sur l'intranet de l'entreprise.

7 Nous empruntons ce terme à CHARBONNEAU, qui a intitulé un commentaire d'arrêt sur la communication syndicale par Internet « Publications et tracts syndicaux dématérialisés ».

8 NORDMANN, plädoyer 1995, p. 45, et MÜLLER, p. 204, citent, comme services administratifs, divers travaux de secrétariat (dactylographie, procès-verbaux, impression, envois).

9 Expression empruntée à DESCHENAUX, p. 81.

Tout d'abord, Internet et l'intranet sont compris dans l'esprit[10] de l'article 11 al. 2 2e phrase Loi sur la participation et entrent dans son champ d'application[11]. En effet, la mise à disposition de ces réseaux n'est pas sans rapport avec la *ratio legis* de l'article 11 Loi sur la participation : donner à la représentation des travailleurs les moyens d'exercer les droits de participation prévus par la loi. Comme le précise le Conseil fédéral, le soutien de l'employeur constitue « l'une des conditions préalables dont dépend l'exercice des droits de participation »[12]. En ce sens, la mise à disposition d'Internet et de l'intranet peut servir à l'accomplissement des fonctions de représentation des travailleurs et participer ainsi à l'objectif visé par cette disposition. Tous les moyens répondant à ce but ne sont cependant pas compris dans la liste de l'article 11 Loi sur la participation. Le législateur a limité sa liste à des catégories de moyens par lesquels l'employeur soutient la représentation des travailleurs « en nature ». Un soutien financier, « en espèces », sortirait du cadre tracé par le législateur. Or, l'utilisation d'Internet et de l'intranet relève plutôt d'un soutien en nature. De plus, ces réseaux représentent une nouvelle génération de moyens d'information et de communication (destinés à compléter, voire à se substituer au papier ou au téléphone) et ne sont pas très éloignés des moyens énumérés dans la loi.

Par conséquent, la mise à disposition d'Internet et de l'intranet entre dans le champ d'application de l'article 11 al. 2 2e phrase Loi sur la participation. Cela signifie que la représentation élue des travailleurs a le droit d'exiger de l'employeur l'accès et l'utilisation de ces réseaux, dans la mesure nécessaire à l'exercice de ses tâches.

2. Condition

L'article 11 al. 2 2e phrase Loi sur la participation soumet l'obligation de l'employeur de mettre des moyens à disposition de la représentation des travailleurs à la condition de nécessité. Ainsi, la mesure dans laquelle le droit des représentants élus d'utiliser Internet et l'intranet dans l'entreprise dépend de la nécessité de ces moyens.

Cette appréciation de la nécessité doit se faire au cas par cas, en fonction des circonstances concrètes. Nous proposerons quelques points de repères eu égard à Internet et à l'intranet (voir *infra* III).

---

10 Art. 1 al. 1 CC : « la loi régit toutes les matières auxquelles se rapportent la lettre ou l'esprit de l'une de ses dispositions ».

11 ROSENTHAL, p. 369-370, repris par HOLENSTEIN, p. 52, admet l'application de l'art. 11 al. 2 Loi sur la participation à un moyen de communication électronique.

12 Message du CF du 15 juin 1992, FF 1992 V 632.

A ce stade, il convient de définir la notion de nécessité (« notwendig » dans la version allemande).

Premièrement, pour qu'un moyen soit considéré comme nécessaire, il ne suffit pas qu'il soit utile. L'application du principe de la proportionnalité le montre bien, puisqu'elle comprend d'abord l'examen de l'aptitude – comparable à ce qui est utile au but recherché –, puis celui de la nécessité.

Deuxièmement, un moyen n'est nécessaire que s'il est indispensable[13]. Dans le cadre de l'application de l'article 11 al. 2 Loi sur la participation, cette appréciation relativement restrictive du terme « nécessaire » se justifie pour plusieurs raisons. Tout d'abord, la Loi sur la participation est une loi-cadre, qui appelle une concrétisation par les partenaires sociaux[14]. Le titre marginal de son article 11, « principe », le rappelle. Ensuite, l'étendue des moyens nécessaires à l'exercice des tâches de la représentation élue est fonction de celle des droits de participation de cette entité – or, dans l'ordre juridique suisse, ces droits sont relativement restreints[15]. Enfin, l'utilisation d'Internet et de l'intranet de l'entreprise par les représentants élus des travailleurs ne semble pas encore faire partie du minimum reconnu par les partenaires sociaux, puisque aucune convention collective ne l'évoque[16]. Il s'agit donc de respecter le choix du législateur et le système de fonctionnement du droit collectif suisse du travail en n'imposant pas aux entreprises d'accorder à la représentation élue des travailleurs des moyens qui iraient au-delà de ce qui est indispensable. D'ailleurs, en matière de droits syndicaux, le Tribunal fédéral utilise le même critère, appréciant la licéité du droit d'accès à l'entreprise en fonction de ce qui est « indispensable » ou non à l'exercice de la liberté syndicale[17]. Cette interprétation est compatible avec le but de l'article 11 al. 2 Loi sur la participation, qui est de rendre possible l'exercice des droits de la représentation élue des travailleurs à l'information et à la consultation[18].

---

13 Voir la définition de « nécessaire » donnée par le Larousse : « dont la présence ou l'action rend seule possible une fin, un effet ; dont on ne peut se passer ; qui est très utile ou obligatoire, indispensable, qui doit être fait, qui s'impose ».

14 BOCN 1992, p. 1451-1452.

15 A cet égard, il est utile de comparer les art. 9 et 10 Loi sur la participation avec les § 74 à 113 BetrVG en droit allemand ou les art. L. 2323-1 à L. 2323-87 CT en droit français.

16 Selon nos recherches sur les conventions collectives applicables à Genève, http://www.ge.ch/ocirt (consulté le 10 décembre 2013).

17 « Un droit d'accès à l'entreprise ne s'interprète pas comme étant une composante indispensable de la liberté syndicale consacrée par l'art. 28 Cst. » (TF 6B_758/2011 du 24 septembre 2012, consid. 1.3.4).

18 Voir Message du CF du 15 juin 1992, FF 1992 V 632.

Troisièmement, comme le souligne un auteur, la condition de la nécessité signifie notamment que la mise à disposition ne doit être ni disproportionnée ni excessive[19]. Il s'impose donc de prendre en considération non seulement l'intérêt de la représentation élue des travailleurs, mais aussi celui de l'employeur.

En résumé, un moyen sera nécessaire au sens de l'article 11 Loi sur la participation à une triple condition : s'il sert à l'exercice des tâches de la représentation élue des travailleurs, qu'il lui soit indispensable – c'est-à-dire que sans ce moyen la représentation ne pourrait accomplir ses tâches – et que la mise à disposition ne demande pas à l'employeur un effort disproportionné par rapport à l'avantage qu'en retirera la représentation élue.

B. Syndicats

La Constitution garantit la liberté syndicale[20] qui comprend notamment le droit, tant pour le syndicat que pour ses membres, d'exercer une activité syndicale[21].

Concrétisant cette garantie constitutionnelle, le Code des obligations contient, outre un chapitre sur les conventions collectives de travail[22], un seul article sur le droit syndical[23].

Dans ce contexte, il convient d'examiner brièvement dans quelle mesure les salariés syndiqués, respectivement le syndicat représenté par des syndicalistes non employés dans l'entreprise, ont le droit d'exercer une activité syndicale dans l'entreprise.

1. Salariés syndiqués

L'article 336 al. 2 let. a CO déclare abusif le licenciement donné pour cause d'exercice conforme au droit d'une activité syndicale. Il résulte des décisions rendues sur la base de cette disposition que constituent des activités syndicales licites la mise à disposition de brochures ou l'affichage dans les bureaux du personnel, pour autant qu'aucune obligation découlant du contrat de travail ou d'une convention collective ne soit violée[24]. En parti-

19 FRITZ, p. 40.
20 Art. 28 Cst.
21 GARRONE, p. 797.
22 Art. 356 ss CO.
23 Art. 336 al. 2 let. a CO.
24 Voir par exemple Cour civile du Tribunal cantonal de Fribourg, 19 janvier 1998, RFJ 1998, p. 70 ; Chambre d'appel des prud'hommes du Canton de Genève, 18 avril 2002, JAR 2003, p. 283. Voir aussi Message du CF du 9 mai 1984, FF 1984 II 625 ; STREIFF/VON KAENEL/RUDOLPH, N 11 ad art. 336 CO ; SUBILIA/DUC, N 43 ad art. 336 CO ; BRUNNER/BÜHLER/WAEBER/BRUCHEZ, N 9 ad art. 336 CO ; STAEHELIN/VISCHER, N 30 ad art. 336 CO.

culier, le bon déroulement du travail ne doit pas être dérangé[25]. Selon la jurisprudence, l'employeur a le droit de restreindre l'exercice de l'activité syndicale, mais pas celui de l'interdire[26]. La bonne marche de l'entreprise et les rapports avec la clientèle constituent des intérêts de nature à justifier la restriction de l'exercice de l'activité syndicale dans l'entreprise[27]. Par conséquent, il nous semble que l'employeur, pour autant qu'il n'empêche pas le syndicat de se faire connaître et d'informer les travailleurs, est autorisé à proscrire l'utilisation des moyens de production de l'entreprise – y compris Internet et l'intranet – à des fins syndicales.

2. Syndicalistes non employés dans l'entreprise

La protection du syndicat lui-même, représenté par des syndicalistes qui ne travaillent pas dans l'entreprise, est assurée par la prise en compte de la liberté syndicale lors de l'application de normes relatives aux intérêts de l'employeur. En effet, les tribunaux doivent veiller à la réalisation des droits fondamentaux, dans la mesure où ils s'y prêtent[28]. Ainsi, dans le cadre de l'interprétation de la loi[29], la liberté syndicale peut servir de base à une discussion l'opposant à la garantie de la propriété (art. 26 al. 1 Cst. concrétisé en droit privé à l'art. 641 CC) ou la liberté économique de l'employeur (art. 27 Cst. concrétisé en droit privé à l'art. 27 CC).

Cependant, faute de réglementation *ad hoc* dans l'ordre juridique suisse, le Tribunal fédéral a nié l'existence d'un droit d'accès du syndicat à l'entreprise qui reposerait directement sur l'art. 28 Cst. – en tout cas hors du contexte d'une grève licite[30]. Par conséquent, en l'état actuel du droit suisse, il faut admettre que les syndicalistes non employés dans l'entreprise n'ont le droit d'y accéder qu'avec l'accord de l'employeur.

Qu'en est-il de l'accès électronique à l'entreprise ? Dans le même arrêt, le Tribunal fédéral reprend les constatations de fait de la Cour cantonale selon laquelle l'envoi de courriels aux salariés aurait constitué un moyen moins incisif que le dépôt de tracts sur les

25 ANDERMATT, N 23.

26 Arbeitsgericht Zürich, 25 octobre 1983, plädoyer 2/84, p. 28.

27 Chambre d'appel des prud'hommes du Canton de Genève, 18 avril 2002, JAR 2003, p. 284 ; DUNAND, N 57 ad art. 336 CO ; WYLER, p. 549.

28 Art. 35 al. 3 Cst. : « Les autorités veillent à ce que les droits fondamentaux, dans la mesure où ils s'y prêtent, soient aussi réalisés dans les relations qui lient les particuliers entre eux ».

29 Voir ATF 132 III 122 (blocage de l'accès à l'entreprise par un syndicat) relatif à l'interprétation de l'art. 41 CO et TF 6B_758/2011 du 24 septembre 2012 (distribution de tracts, par un syndicat, sur les parkings de l'entreprise) relatif à l'interprétation de l'art. 14 CP.

30 TF 6B_758/2011 du 24 septembre 2012, consid. 1.3.4.

voitures situées dans les parkings de l'entreprise destinés aux clients et au personnel[31]. Notre Haute Cour ne s'attarde cependant pas sur cette hypothèse.

III. Questions particulières

A. Affichage sur l'intranet

1. Représentants élus

Les représentants élus du personnel ont-ils le droit d'afficher des informations sur l'intranet de l'entreprise ?

a) Conditions

Il s'agit ici de déterminer dans quelle mesure cet affichage électronique est nécessaire à l'exercice de ses tâches par la représentation élue des travailleurs. Plusieurs éléments entrent en considération.

aa) Equipement informatique de l'entreprise

Tout d'abord, il faut que l'entreprise soit équipée d'un intranet.

bb) Usage de l'intranet dans l'entreprise

Ensuite, le fait que la communication dans l'entreprise passe principalement par l'intranet joue en faveur de l'utilisation de l'intranet par les représentants des travailleurs[32].

cc) Proportion de travailleurs ayant accès à l'intranet dans l'entreprise

De même, la proportion de salariés travaillant avec des ordinateurs dans l'entreprise constitue un facteur d'appréciation de la nécessité de l'affichage sur l'intranet. Ainsi, dans une entreprise du secteur secondaire dont la plupart des employés sont occupés à la production, devant des machines et non assis à un bureau devant un ordinateur, il est plus

31 *Ibidem,* consid. 2.

32 Cet argument a été utilisé en droit allemand (Arbeitsgericht Paderborn, 29 janvier 1998, 1 BV 35/97, http://www.online-recht.de (consulté le 10 décembre 2013) ; Bundesarbeitsgericht (BAG), 3 septembre 2003, 7 ABR 12/03, AP n° 78 ad § 40 BetrVG 1972, consid. B.I.2.c)bb) ; BAG, 1er décembre 2004, 7 ABR 18/04, AP n° 82 ad § 40 BetrVG) et nous semble tout à fait pertinent en droit suisse.

naturel que la communication passe par la voie traditionnelle du panneau d'affichage. En revanche, la représentation élue des travailleurs d'une entreprise dans laquelle 500 des 644 postes de travail (soit 77%) sont équipés d'un accès à l'intranet pourra plus facilement exiger d'utiliser ce réseau[33]. *A fortiori*, le comité d'une entreprise dans laquelle plus de 90% des travailleurs ont accès à l'intranet pourra arguer de ce fait pour obtenir lui aussi d'accéder à ce réseau[34].

dd) Secteur d'activités et taille de l'entreprise

La nécessité de l'affichage sur l'intranet dépend aussi du secteur d'activités et de la taille de l'entreprise : elle s'impose a priori davantage dans une grande entreprise active dans le secteur des hautes technologies que dans une entreprise du bâtiment employant 10 personnes.

ee) Configuration de l'entreprise

Cette nécessité paraît enfin donnée lorsque l'entreprise compte de nombreux travailleurs n'ayant pas souvent accès aux panneaux d'affichage traditionnels (télétravailleurs ou travailleurs itinérants exerçant leur activité principalement en dehors de l'entreprise, où ils ne se rendent que rarement) mais pouvant accéder facilement à l'intranet.

b) Modalités

La nécessité de l'affichage sur l'intranet dépend encore de certaines modalités.

aa) Coûts

Premièrement, il convient que les éventuels coûts engendrés par cet affichage soient limités autant que possible.

bb) Etendue de l'affichage

Deuxièmement, l'étendue de l'affichage (simple rubrique ou véritable site sur l'intranet) doit être adaptée aux circonstances. L'employeur peut craindre que plus les représentants

---

33 Exemple tiré de la jurisprudence allemande (BAG, 3 septembre 2003, 7 ABR 12/03, consid. B.I.2.c)bb)) – l'argument nous semble pertinent en droit suisse aussi ; cela ne signifie cependant pas que l'ensemble des considérations et du dispositif de cet arrêt pourrait être « importé » en droit suisse.

34 Exemple tiré de la jurisprudence allemande (BAG, 1er décembre 2004, 7 ABR 18/04) – même remarque qu'à la note précédente.

affichent d'informations sur l'intranet, plus les salariés passent du temps à les lire, le cas échéant au détriment de l'accomplissement de leur travail. En Allemagne, dans une affaire où le comité de l'établissement central d'une grande entreprise réclamait de publier lui-même des informations sur l'intranet de celle-ci – réseau accessible à partir de toutes les succursales –, l'employeur objecta que les salariés des autres établissements liraient des nouvelles qui ne les concerneraient pas, à savoir celles publiées par le comité de l'établissement central, au détriment de l'accomplissement de leur travail. Le Tribunal fédéral allemand du travail écarta cette objection, jugeant qu'il appartenait à l'employeur de prendre des mesures (d'ordre technique ou disciplinaire) pour éviter qu'il en soit ainsi. Prenant également d'autres éléments en considération, la Haute Cour conclut que le comité de l'établissement central avait le droit à une page sur l'intranet de l'entreprise[35].

cc) Contenu

Troisièmement, les informations publiées sur l'intranet par la représentation élue des travailleurs doivent être en rapport avec ses tâches telles que prévues par la Loi sur la participation. Ainsi, les représentants ont le droit de donner aux travailleurs des informations sur leurs activités, de leur communiquer les comptes-rendus de leurs réunions et de les consulter, par exemple, au moyen de questionnaires en rapport avec leurs tâches. Ils restent en tous les cas liés par une obligation de discrétion applicable aux affaires personnelles des travailleurs ainsi qu'aux affaires pour lesquelles l'employeur ou la représentation des travailleurs l'exige expressément sur la base d'intérêts légitimes (art. 14 al. 2 Loi sur la participation).

En outre, eu égard au contenu, les trois questions suivantes méritent d'être traitées.

Les représentants élus auraient-ils le droit d'afficher des informations syndicales ou de prévoir un lien de l'intranet de l'entreprise vers un site syndical ? Sauf autorisation de l'employeur, les représentants élus ne doivent afficher que des informations relatives à leurs tâches. Vu le système de représentation des travailleurs dualiste que connaît la Suisse (représentants élus d'une part, syndicats d'autre part), la publication des informations relatives aux seconds ne fait pas partie des tâches des premiers. Par conséquent, il n'existe pas un droit des représentants élus à communiquer des informations syndicales.

35 BAG, 1er décembre 2004, 7 ABR 18/04. *In casu*, le comité central de l'entreprise bénéficiait, en vertu d'un accord collectif passé entre lui-même et l'employeur, du droit d'affichage sur l'intranet de l'entreprise. Cet accord permettait en outre au comité central de l'entreprise de mettre cet intranet à disposition des comités d'établissement.

L'employeur a-t-il le droit de donner son accord sur le contenu des informations préalablement à leur diffusion sur l'intranet ? L'interdiction faite à l'employeur d'empêcher[36] un membre de la représentation élue d'exercer son activité ou de discriminer un représentant élu des travailleurs (art. 12 Loi sur la participation) a notamment pour but de permettre à la représentation élue d'agir de manière libre et responsable[37]. Cette indépendance de la représentation élue des travailleurs, de même que l'obligation de l'employeur et de cette dernière de collaborer de bonne foi (art. 11 al. 1 Loi sur la participation), entraînent l'interdiction, pour l'employeur, de censurer les informations émanant de cet organe.

Les représentants élus ayant le droit de déterminer eux-mêmes quelles informations seront publiées sur leur page intranet, il importe peu, du point de vue juridique, qu'ils insèrent eux-mêmes ces informations ou que cette tâche revienne à un auxiliaire de l'employeur, par exemple un webmaster. S'occuper de la maintenance de leur page sur l'intranet répond à un intérêt pratique, celui d'avoir une plus grande maîtrise du moment auquel les modifications sont effectivement apportées. L'employeur peut cependant préférer confier cette tâche à son webmaster, afin de concentrer en une seule personne les interventions sur l'intranet. Il évite ainsi de fausses manœuvres ou un manque de cohérence.

2. Syndicats

Les syndicats ont-ils le droit d'afficher ou de faire afficher des informations sur l'intranet de l'entreprise ?

A titre liminaire, il convient de préciser que seuls des salariés syndiqués peuvent avoir le droit d'afficher des informations sur l'intranet. En effet, si les syndicats eux-mêmes n'ont

---

36 L'art. 12 al. 1 Loi sur la participation interdit à l'employeur d'empêcher (« behindern ») les représentants des travailleurs d'exercer leur mandat. En droit allemand, le § 78 BetrVG interdit non seulement d'empêcher (« behindern ») mais aussi de troubler (« stören »). On ne peut déduire de cette comparaison que le droit suisse n'interdirait que l'empêchement mais permettrait à l'employeur de seulement troubler l'activité des représentants des travailleurs. Un commentateur de la Loi sur la participation se demande si l'art. 12 al. 1 de cette loi n'est pas superflu, puisque la protection qu'il prévoit découle de l'obligation de collaborer de bonne foi (art. 11 al. 1 Loi sur la participation) et de l'interdiction de discriminer les représentants élus (art. 12 al. 2 Loi sur la participation) (FRITZ, p. 41). De ces prescriptions résulte, à notre avis, non seulement l'interdiction d'empêcher les représentants élus d'accomplir leur mandat, mais aussi de le troubler. La doctrine suisse semble partager ce point de vue (ILG, p. 86 et MÜLLER, p. 80 utilisent le terme « Beeinträchtigung », soit trouble ; NORDMANN, Dossier USS, p. 18, parle même de l'interdiction de rendre l'activité des représentants des travailleurs plus difficile (« erschweren »)).

37 Voir ILG, p. 86.

pas le droit de pénétrer physiquement dans l'entreprise[38], la loi ne leur permet pas non plus d'y accéder virtuellement. Cela vaut d'autant plus que l'intranet procure un accès libre à davantage d'informations.

En l'absence de texte législatif et de jurisprudence topiques, il convient d'effectuer une comparaison avec la pratique relative aux panneaux d'affichage.

En droit suisse, aucune disposition légale n'oblige l'employeur à fournir des panneaux d'affichage traditionnels aux syndicats. Cette pratique est cependant répandue : elle apparaît dans plusieurs conventions collectives[39] – l'affichage nécessitant parfois l'accord de l'employeur[40] –, ainsi que dans la fonction publique genevoise[41]. La transposer à l'intranet relève du libre choix de l'employeur, propriétaire des lieux et des ordinateurs. A Genève, il a été question d'octroyer aux syndicats de la fonction publique le

38 TF 6B_758/2011 du 24 septembre 2012, consid. 1.3.4.

39 Art. 23.3 CCT genevoise aide et soins à domicile, conclue entre l'IMAD d'une part, le SSP-VPOD et le SIT d'autre part, valable du 1er janvier 1995 au 31 décembre 2010, reconduite ; art. 51 al. 8 CCT genevoise animateurs, conclue entre la FASe d'une part, le SSP-VPOD et le SIT d'autre part, entrée en vigueur le 1er janvier 2004 et reconduite tacitement d'année en année ; art. 3.7 al. 5 CCT genevoise EMS, conclue entre la Fegems d'une part, Unia, l'ASI, le SIT, le SSP-VPOD et Syna d'autre part, valable du 1er janvier 2010 au 31 décembre 2014 ; art. 46 al. 7 CCT genevoise du personnel des institutions de la petite enfance, conclue entre la Ville de Genève, Délégation à la petite enfance et la Fédération genevoise des institutions de la petite enfance d'une part, le SIT, le SSP-VPOD, l'Association genevoise des cadres des institutions de la petite enfance genevoise et l'Association genevoise des éducatrices et éducateurs du jeune enfant d'autre part, entrée en vigueur le 1er janvier 2007 et reconduite tacitement d'année en année. Toutes ces conventions collectives se trouvent sur : http://www.ge.ch/ocirt (consulté le 10 décembre 2013).

40 Art. 4.6 al. 7 CCT horlogerie, conclue entre la Convention patronale de l'industrie horlogère suisse et Unia, même convention avec Syna, valable du 1er janvier 2012 au 31 décembre 2016 – l'affichage est soumis à l'accord préalable de la direction ; art. 23 CCT genevoise de l'industrie des garages, conclue entre l'UPSA et Unia, valable du 1er janvier 2009 au 31 décembre 2011, reconduite tacitement d'année en année – l'affichage est soumis à l'accord de l'employeur ; art. 20 CCT genevoise transports et déménagements, conclue entre l'association genevoise des entreprises de transport et l'association genevoise des entreprises de déménagements d'une part, Unia d'autre part, valable du 1er janvier 2013 au 31 décembre 2013 – le texte doit préalablement être soumis au secrétariat des associations patronales signataires ; art. 1.08 CCT genevoise installateur en chauffage, ventilation et climatisation, conclue entre l'Association genevoise des entreprises de chauffage et de ventilation d'une part, Unia d'autre part, valable du 1er février 2011 au 31 décembre 2013, puis reconduite tacitement d'année en année, étendue à toute la branche, RS-GE J 1 50.27 – les textes doivent préalablement être soumis à l'approbation de l'employeur ; les trois CCT genevoises applicables aux ferblantiers, aux serruriers et aux monteurs électriciens contiennent la même disposition (RS-GE J 1 50.28, 50.29 et 50.26).

41 Art. 18 al. 1 à 4 du Règlement d'application de la Loi générale relative au personnel de l'administration cantonale et des établissements publics médicaux du 24 février 1999, RS-GE B 5 05.01.

droit d'afficher des informations sur une page spécifique de l'intranet de l'Etat ; cette proposition n'a pas été retenue[42].

Par conséquent, sauf accord de l'employeur ou convention collective le prévoyant expressément, l'affichage syndical sur l'intranet n'est pas licite.

B. Messagerie électronique dans l'entreprise

Les représentants du personnel, élus et syndicaux, ont-ils le droit d'informer et de communiquer avec les travailleurs au moyen de la messagerie électronique professionnelle ?

1. Représentants élus

a) Conditions

S'agissant de la messagerie électronique, l'application de la condition de nécessité par la doctrine se traduit comme suit : l'employeur qui interdirait l'usage de la messagerie électronique, alors qu'elle constitue le seul moyen approprié de communication entre les représentants des travailleurs et le personnel, violerait l'article 11 al. 2 Loi sur la participation[43]. Or, la situation actuelle, appelée à perdurer, voit coexister différents moyens de communication (rencontres, courrier papier, téléphone, fax et Internet). La messagerie électronique offre de nombreux avantages, mais ne constitue pas le seul moyen de communication entre les travailleurs et leurs représentants. Par conséquent, sauf urgence ou cas particulier rendant le recours au courrier postal inapproprié, l'employeur n'a, à notre avis, pas l'obligation de permettre aux représentants élus d'utiliser la messagerie électronique.

b) Modalités

aa) Contenu

Les courriels envoyés par les représentants élus des travailleurs se rapporteront en principe aux objets soumis à la consultation. De même, les représentants des travailleurs pourront transmettre au personnel les informations qu'ils ont reçues de la direction – en respectant leur devoir de discrétion (art. 14 al. 2 Loi sur la participation).

---

42 Mémorial du Grand Conseil genevois, 54e législature, 4e année, session 7, 6 avril 2001, séances 18 et 19.

43 ROSENTHAL, p. 369-370 ; HOLENSTEIN, p. 51.

bb) Envoi en masse

La limitation, voire l'interdiction, des envois en masse répond au souci de ne pas surcharger le réseau informatique de l'entreprise. Elle a aussi pour but d'éviter les abus.

Ces intérêts de l'employeur se heurtent à ceux de la représentation élue des travailleurs. Celle-ci a vocation à représenter l'ensemble du personnel, il est donc nécessaire que ses messages atteignent tous les travailleurs qu'elle représente. Même si la loi ne le précise pas, les représentants ont à notre avis le droit de consulter en tout temps ceux qu'ils représentent, afin de remplir leur tâche au plus près des intérêts des travailleurs. Reste à définir le moyen de l'information ou de la consultation.

La condition de la nécessité posée par l'article 11 Loi sur la participation implique que l'envoi en masse soit réservé à des cas particuliers : urgence ou économie en termes de coûts rendant nécessaire l'envoi de messages collectifs en lieu et place d'un autre mode de communication.

cc) Liste d'adresses

Lorsque les représentants élus ont le droit d'envoyer un message à tous ou à certaines catégories de travailleurs, il se pose la question de l'utilisation d'une liste regroupant les adresses de ces salariés.

Il se peut que les représentants configurent la messagerie de façon à bénéficier d'une fonction permettant l'envoi de courriels collectifs – ce qui, du point de vue de l'employeur, ne pose pas de problème s'il a autorisé l'envoi en masse ou que ce dernier soit nécessaire au sens de l'article 11 Loi sur la participation.

En outre, si cela s'avère nécessaire au sens de l'article 11 al. 2 Loi sur la participation et qu'aucune autre loi ne s'y oppose[44], les représentants élus pourraient avoir le droit d'exiger de l'employeur qu'il leur remette une liste des adresses électroniques professionnelles des travailleurs qu'ils représentent.

A cet égard, il convient d'examiner si les dispositions sur la protection des données limitent la transmission, par l'employeur, d'une liste des adresses de ses salariés à leurs représentants élus.

Dans la mesure où elles sont nominatives (prénom.nom@entreprise.ch, par exemple), les adresses professionnelles des salariés constituent des données personnelles. A ce titre, le salarié peut-il demander que son adresse électronique professionnelle ne soit pas communiquée à l'organe de représentation élue du personnel ? L'article 328*b* CO limite le

44 Voir *infra* nos développements relatifs à la Loi sur la protection des données.

traitement de données personnelles par l'employeur à celles qui portent sur les aptitudes du travailleur à remplir son emploi ou qui sont nécessaires à l'exécution du contrat de travail ; il renvoie en outre à la Loi sur la protection des données (LPD)[45]. Celle-ci protège la personnalité et notamment le droit de déterminer l'usage des données personnelles[46]. Constitue une atteinte à la personnalité un traitement de données qui est à la fois contraire aux principes de la protection des données et dénué de motif justificatif[47]. En particulier, en l'absence de motif justificatif, un traitement est illicite s'il n'est pas reconnaissable pour la personne concernée[48]. Cependant, un traitement conforme aux principes énoncés à l'art. 4 LPD est licite[49]. Ainsi, traiter une donnée personnelle conformément au but qui ressort des circonstances ne constitue pas une atteinte à la personnalité. S'agissant d'adresses professionnelles, il est évident qu'elles peuvent être utilisées dans le cadre de l'entreprise. Le salarié ne pourra pas s'opposer à un tel traitement. Plus particulièrement, on ne voit pas ce qui s'oppose à la diffusion de cette adresse à l'intérieur de l'entreprise, puisque c'est dans ce cadre que cette adresse a sa raison d'être. Les représentants élus des travailleurs font partie de l'entreprise et ont des compétences reconnues par la loi. Par conséquent, ils ont le droit de recevoir une liste des adresses professionnelles des salariés qu'ils représentent. L'utilisation de l'adresse professionnelle à l'intérieur de l'entreprise constitue donc un traitement licite.

2. Salariés syndiqués

Les salariés syndiqués ont-ils le droit d'envoyer à leurs collègues des messages électroniques à caractère syndical en utilisant la messagerie mise à disposition par l'employeur ?

a) Absence de réglementation

En l'absence de convention collective ou de réglementation d'entreprise relative à l'utilisation syndicale de la messagerie électronique dans l'entreprise, il convient d'en juger à l'aune de « l'activité syndicale conforme au droit » au sens de l'article 336 al. 2 let. a CO.

La jurisprudence relative à cette disposition ne concerne que les moyens de communication traditionnels (mise à disposition de brochures, affichage dans les bureaux du person-

45 Loi fédérale sur la protection des données (LPD) du 19 juin 1992, RS 235.1.
46 Message du CF du 23 mars 1988, FF 1988 II 426.
47 MEIER, N 1536 et 1539 ; MAURER-LAMBROU/KUNZ, N 9 ad art. 1 LPD.
48 MEIER, N 649.
49 Voir notamment art. 4 al. 3 LPD : « 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 ».

nel[50], distribution d'un tract syndical convoquant les travailleurs à une assemblée générale[51]). Il en ressort que, pour être conforme au droit, l'activité syndicale ne doit notamment ni affecter la qualité du travail ni donner lieu à des plaintes de la part des clients[52].

Par conséquent, en l'absence de convention collective ou de directive de l'employeur, l'utilisation de la messagerie électronique professionnelle à des fins syndicales pourrait, selon les circonstances (bref message urgent aux membres du syndicat, par exemple) être considérée comme licite. Faute de réglementation du droit syndical dans l'entreprise en droit suisse (à part l'article sur le congé abusif) et en raison de la prépondérance de la négociation collective sur la législation en matière de droit collectif du travail suisse, il se justifie de n'admettre un tel droit que de manière restrictive, dans la mesure où les salariés peuvent également être atteints d'une autre manière que par la messagerie électronique professionnelle (conversation pendant les pauses, messagerie électronique privée, téléphone portable privé, courrier papier), sans recours aux ressources mises à disposition par l'employeur.

b) Directive ou convention collective

Lorsque l'employeur émet des directives, la licéité de l'activité syndicale dans l'entreprise est subordonnée au respect de celles-ci[53]. Au vu de la jurisprudence rappelée *supra*[54], il nous semble que l'employeur, pour autant qu'il n'empêche pas le syndicat de se faire connaître et d'informer les travailleurs, est autorisé à proscrire l'utilisation de la messagerie électronique de l'entreprise à des fins syndicales.

Précisons que l'utilisation privée ne se confond pas avec l'utilisation syndicale. Ainsi, on ne peut présumer que l'employeur qui émet des directives sur l'utilisation de la messagerie électronique à des fins privées entende régler aussi l'utilisation de cette messagerie à des fins syndicales. En effet, l'utilisation syndicale, même si elle ne constitue pas l'objet de la relation de travail, s'y rapporte directement. Une réglementation de l'utilisation

---

50 Voir par exemple Chambre d'appel des prud'hommes du Canton de Genève, 18 avril 2002, JAR 2003, p. 282-287 ; Bezirksgericht Bülach, 22 décembre 1994, Employeur suisse 1995, p. 719.

51 Chambre d'appel des prud'hommes du Canton de Genève, 20 avril 1988, JAR 1990, p. 238. Antérieur à l'introduction des dispositions sur le congé abusif (art. 336 ss CO), ce jugement s'appuie sur l'interdiction générale de l'abus de droit énoncée à l'art. 2 al. 2 CC. Il est le premier à reconnaître comme abusif un licenciement prononcé en raison de l'exercice d'une activité syndicale.

52 Bezirksgericht Bülach, 22 décembre 1994, Employeur suisse 1995, p. 719.

53 Voir par exemple Cour civile du Tribunal cantonal de Fribourg, 19 janvier 1998, RFJ 1998, p. 70 ; Chambre d'appel des prud'hommes du Canton de Genève, 18 avril 2002, JAR 2003, p. 283. Voir aussi Message du CF du 9 mai 1984, FF 1984 II 625 ; SUBILIA/DUC, N 43 ad art. 336 CO ; BRUNNER/BÜHLER/WAEBER/BRUCHEZ, N 9 ad art. 336 CO ; STAEHELIN/VISCHER, N 30 ad art. 336 CO.

54 Voir *supra* p. 212.

privée ne constitue donc pas (sauf volonté contraire de l'employeur, reconnaissable pour les salariés) une directive relative à l'utilisation à des fins syndicales.

En conclusion, sauf accord de l'employeur ou convention collective la prévoyant expressément, l'utilisation de la messagerie professionnelle à des fins syndicales n'est en principe pas licite.

C. Messagerie électronique de et vers l'entreprise

1. Représentants élus

Les représentants élus du personnel ont-ils le droit de communiquer à l'externe au moyen de la messagerie électronique professionnelle ?

Conformément à l'article 11 al. 2 Loi sur la participation, les représentants élus des travailleurs n'ont le droit de communiquer à l'externe au moyen de la messagerie électronique professionnelle que si cela est nécessaire à l'exercice de leurs tâches.

S'agissant de contacts avec les autorités dans le cadre d'une procédure de consultation en cas de licenciement collectif, la nécessité de l'usage de la messagerie électronique, plutôt que du téléphone ou du courrier papier, peut se justifier par le besoin d'une réponse écrite ainsi que par la brièveté du délai dans lequel la représentation élue doit répondre à l'employeur.

Par conséquent, dans certaines circonstances, l'employeur doit permettre à la représentation élue de communiquer avec des tiers externes à l'entreprise au moyen de la messagerie électronique professionnelle.

2. Syndicats

Les syndicats ont-ils le droit d'envoyer des courriels d'information syndicale aux adresses professionnelles des salariés d'une entreprise ?

En règle générale, les syndicalistes non employés dans l'entreprise n'ont le droit d'y accéder qu'avec l'accord de l'employeur[55]. L'accès physique n'est cependant pas tout à fait comparable à l'envoi de courriels par des personnes extérieures à l'entreprise. Tout d'abord, les risques liés à la divulgation de secrets de l'entreprise lors d'une visite syndicale disparaissent lors de l'envoi de courriels ; il en va de même du risque que la clientèle soit importunée par l'action syndicale. Ensuite, l'employeur a le droit d'interdire

55 TF 6B_758/2011 du 24 septembre 2012, consid. 1.3.4.

l'accès physique à son entreprise ou de défendre à ses employés d'envoyer des courriels syndicaux, mais il n'est pas autorisé à donner des directives à des personnes extérieures à l'entreprise.

Dans l'un de ses arrêts, le Tribunal fédéral mentionne l'envoi de messages électroniques par un syndicat, mais ne se prononce pas sur la licéité d'un tel acte[56]. L'affaire concernait le dépôt de tracts, par des secrétaires syndicaux, sur les véhicules stationnés dans les parkings réservés aux clients et aux employés d'un restaurant. Au cours de son analyse, le Tribunal fédéral rapporte les constatations de fait de la Cour cantonale, selon laquelle le syndicat avait d'autres moyens moins incisifs que ladite distribution de tracts : il aurait pu demander à l'employeur la liste de ses « employés afin de les contacter par courrier postal ou électronique » ou se poster sur la voie publique, à proximité immédiate des terrains de l'employeur[57]. Ni la Cour cantonale ni le Tribunal fédéral ne précisent s'il s'agit des adresses professionnelles ou privées des travailleurs.

A cet égard, il convient de se demander si l'employeur a le droit, voire l'obligation, de fournir au syndicat une liste de ses employés, respectivement de leurs adresses électroniques.

Vis-à-vis du syndicat, l'employeur peut faire valoir ses propres intérêts (garder pour lui la liste de ses salariés, ne pas risquer que ces derniers soient dérangés dans leur travail par des courriels étrangers à leur prestation de travail), mais aussi ceux de ses employés découlant de la protection des données personnelles. En effet, la communication, par l'employeur, de la liste de ses salariés à un syndicat sort du cadre de l'article 328*b* CO (données portant sur les aptitudes du travailleur à remplir son emploi ou qui sont nécessaires à l'exécution du contrat de travail). Aucune base légale ne prévoit une telle communication. Il ne nous semble pas que le salarié doive s'attendre, de bonne foi, à ce que son adresse professionnelle nominative soit communiquée par l'employeur à un syndicat extérieur à l'entreprise (cf. art. 4 LPD). Seul le consentement du salarié pourrait justifier une telle communication ; il serait valable, puisqu'il ne porterait pas sur une dérogation à l'article 328*b* CO défavorable au travailleur (art. 362 CO). Par conséquent, rien n'oblige l'employeur à communiquer à un syndicat la liste de ses salariés.

Par ailleurs, la liberté syndicale négative impose de respecter la volonté du salarié de ne pas recevoir un message syndical ; selon nous, le système de l'*opt-out* (droit du destinataire de refuser tout message ultérieur provenant du même expéditeur) suffit s'agissant de l'envoi d'un courriel par un syndicat, ce dernier n'étant pas comparable à un tiers quelconque.

56 *Ibidem*, consid. 2.
57 *Ibidem*.

A notre avis, l'envoi, par un syndicat, de messages électroniques à tous les salariés d'une entreprise peut, selon les circonstances, constituer un abus de droit – pour autant que ce droit existe. L'admissibilité d'une telle action dépend de l'importance accordée aux droits du propriétaire et titulaire de la liberté économique par rapport à une activité syndicale susceptible d'être exercée par un autre moyen, moins intrusif.

Parmi les circonstances à prendre en considération figure le fait que le syndicat compte déjà des membres parmi les salariés de l'entreprise. Dans ce cas, d'une part le syndicat a la possibilité de traiter directement avec ses membres, d'autre part, grâce à ses membres employés dans l'entreprise, le syndicat a la possibilité de faire passer des informations aux autres salariés. En revanche, lorsqu'il ne compte aucun membre parmi le personnel de l'entreprise, le syndicat n'a pas d'autre alternative que d'informer le personnel par l'intermédiaire de représentants non employés dans l'entreprise. Cela ne signifie pas encore qu'il soit en droit d'envoyer des messages électroniques aux adresses de tous les salariés. Dans la plupart des cas, le syndicat a d'autres moyens d'information. Seul un examen des circonstances concrètes permet de juger de l'admissibilité de l'envoi aux adresses électroniques professionnelles.

IV. Conclusion

Les représentants des travailleurs, élus ou syndicaux, ne bénéficient pas d'un droit absolu à utiliser Internet ou l'intranet dans l'entreprise. L'existence et les modalités d'exercice de ce droit dépendent toujours des circonstances.

Par souci de sécurité juridique, la représentation élue des travailleurs a intérêt à s'entendre préalablement avec l'employeur, étant rappelé que ces deux parties ont l'obligation légale de collaborer de bonne foi.

De même, s'agissant de l'activité syndicale, les parties ont intérêt à s'entendre par le biais de conventions collectives par exemple. En l'absence d'accord, l'affichage syndical sur l'intranet et l'utilisation de la messagerie professionnelle à des fins syndicales ne sont en principe pas licites. Pour autant qu'elle constitue le moyen le moins attentatoire aux intérêts économiques de l'employeur et qu'elle soit indispensable, dans un cas concret, pour informer les salariés de leurs droits ou de l'existence du syndicat, l'utilisation de la messagerie électronique voire de l'intranet, à des fins syndicales, pourrait être considérée comme licite.

Bibliographie

ANDERMATT ARTHUR, Liberté syndicale et droit de grève, in : UNION SYNDICALE SUISSE (édit.), Droit collectif du travail, Bâle 2010, p. 3-52.

BRUNNER/BÜHLER/WAEBER/BRUCHEZ, Commentaire du contrat de travail, 3e éd., Lausanne 2004.

CHARBONNEAU CYRILLE, Publications et tracts syndicaux dématérialisés, Cahiers sociaux du Barreau de Paris, n° 169, avril 2005, p. A 32.

DESCHENAUX HENRI, Le Titre préliminaire du Code civil, Fribourg 1969.

DUNAND JEAN-PHILIPPE, in : DUNAND/MAHON (édit.), Commentaire du contrat de travail, Berne 2013.

FRITZ MAX, La loi sur la participation : commentaire et guides pratiques relatifs à la loi fédérale sur l'information et la consultation des travailleurs dans les entreprises du 17 décembre 1993 ainsi qu'aux modifications touchant le droit du contrat de travail (transfert d'entreprise, licenciement collectif), du 17 décembre 1993, Zurich 1994.

GARRONE PIERRE, La liberté syndicale, in : THÜRER/AUBERT/MÜLLER (édit.), Verfassungsrecht der Schweiz/Droit constitutionnel suisse, Zurich 2001, p. 795-807.

HOLENSTEIN CHRISTOPH, Die Benutzung von elektronischen Kommunikationsmitteln (Internet und Intranet) im Arbeitsverhältnis, Berne 2002.

ILG WALO C., Kommentar über das Bundesgesetz über die Information der Arbeitnehmer in den Betrieben : (Mitwirkungsgesetz), Zurich 1999.

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

MAURER-LAMBROU/KUNZ, in : MAURER-LAMBROU/VOGT (édit.), Datenschutzgesetz, 2e éd., Bâle 2006.

MÜLLER ROLAND A., Die Arbeitnehmervertretung, Berne 1999.

NORDMANN DANIEL, Das schweizerische Mitwirkungsgesetz, Dossier n° 22 de l'Union syndicale suisse, Berne 1994 (cité: NORDMANN, Dossier USS).

NORDMANN DANIEL, La nouvelle loi sur la participation, plädoyer 1995, p. 43-45 (cité : NORDMANN, plädoyer 1995).

ROSENTHAL DAVID, Projekt Internet, Was Unternehmen über Internet und Recht wissen müssen, Zurich 1997.

STAEHELIN/VISCHER, Art. 319-362 CO, Commentaire zurichois, 3e éd., Zurich 1996.

STREIFF/VON KAENEL/RUDOLPH, Arbeitsvertrag, Praxiskommentar zu Art. 319-362 OR, 7e éd., Zurich 2012.

SUBILIA/DUC, Droit du travail – Eléments de droit suisse, Lausanne 2010.

WYLER RÉMY, Droit du travail, 2e éd., Berne 2008.

VINCENT SALVADÉ / NATHALIE TISSOT

La réalisation d'un site web ou l'ouverture d'un compte par le travailleur. Qui est titulaire des droits ?

Sommaire

		Page
I.	La qualification du site Internet en droit d'auteur	228
	A. Introduction	228
	B. Le site Internet est-il un logiciel ?	228
	C. Le site Internet en tant qu'œuvre dérivée ou recueil	229
	D. Le site Internet en tant qu'œuvre collective	230
II.	L'acquisition des droits sur les œuvres préexistantes	231
	A. Introduction	231
	B. Les droits mis en jeu	231
	C. L'acquisition des droits sur les logiciels	233
	D. L'acquisition des droits sur les œuvres littéraires et artistiques préexistantes	234
	1. Le contact des ayants droit individuellement	234
	2. La gestion collective	234
	3. Les licences libres et de libre diffusion	236
III.	L'acquisition des droits sur le site ou sur le compte	237
	A. Introduction	237
	B. Le développement de la plateforme par des employés	238
	1. Le principe du créateur	239
	2. Les logiciels de service, art. 17 LDA	239
	3. L'acquisition à titre dérivé des droits par l'employeur pour les autres catégories d'œuvres	242
	a) L'obligation de rendre compte et de restituer et acte de disposition préalable	243
	b) La théorie de la finalité et l'étendue des droits cédés	247
	c) L'absence de cession des droits moraux	250
	C. La réalisation de la plateforme par des tiers externes	251
IV.	Conclusion	251
V.	Bibliographie	252

I. La qualification du site Internet en droit d'auteur

A. Introduction

Un site Internet est basé sur des logiciels. Ceux-ci sont protégés par le droit d'auteur d'après l'art. 2 al. 3 de la Loi fédérale sur le droit d'auteur et les droits voisins (LDA)[1], s'ils disposent de l'individualité nécessaire. Mais, parallèlement, le site Internet comprendra des images, des textes, des films, parfois de la musique, etc. Ces éléments peuvent avoir la qualité d'œuvres littéraire et artistique au sens de l'art. 2 al. 1 LDA, soit de créations de l'esprit ayant un caractère individuel. Le régime juridique des logiciels et des œuvres littéraires et artistiques n'est pas toujours identique. Notamment, le droit exclusif sur le logiciel n'est pas limité par l'exception d'usage privé au sens de l'art. 19 LDA[2]. Cela a pour conséquence, en particulier, que les droits à rémunération pour l'usage privé, prévus par l'art. 20 LDA, ne sont pas applicables aux logiciels. De même, la durée de protection est de 50 ans dès le décès de l'auteur pour les logiciels, alors qu'elle est de 70 ans dès ce décès pour les œuvres littéraires et artistiques[3]. Enfin, l'art. 17 LDA prévoit que « *l'employeur est seul autorisé à exercer les droits exclusifs d'utilisation sur le logiciel créé par le travailleur dans l'exercice de son activité au service de l'employeur et conformément à ses obligations contractuelles* », alors qu'une telle disposition n'existe pas pour les autres œuvres.

Dans un premier temps, il convient donc de se pencher sur la qualification du site Internet en droit d'auteur.

B. Le site Internet est-il un logiciel ?

D'après l'art. 2 al. 3 LDA, « *les programmes d'ordinateurs (logiciels) sont également considérés comme des œuvres* ». La loi qualifie donc les logiciels de « programmes d'ordinateurs », mais elle ne contient aucune définition de cette notion de « programmes ». Il s'agit d'une omission voulue, c'est-à-dire d'un silence qualifié, l'informatique étant soumise à une évolution rapide[4]. D'après les explications du message, il faut cependant comprendre qu'un programme est un procédé destiné à exécuter certaines tâches ; à l'instar du langage courant, il définit une succession

1 RS 231.1.
2 Art. 19 al. 4 LDA.
3 Art. 29 al. 2 LDA.
4 Message du CF, FF 1993 III 507. A ce sujet, voir HILTY, p. 92.

d'ordres que l'ordinateur exécute pour accomplir une tâche[5]. On ne saurait donc assimiler les sites Internet à de simples logiciels[6] : un site ne contient pas uniquement une succession d'ordres à l'attention de l'ordinateur, il englobe des images, de la musique, des textes, des séquences de films, etc. Un site Internet contient à la fois des logiciels et des œuvres littéraires et artistiques. S'il dispose du caractère individuel nécessaire, il est couvert par la notion d'œuvre au sens de l'art. 2 al. 1 LDA[7]. Il s'agit à notre avis d'une « autre œuvre visuelle ou audiovisuelle » au sens de l'art. 2 al. 2 let. g LDA[8], voire d'une œuvre multimédia *sui generis*[9] (ce qui est possible puisque la liste de l'art. 2 al. 2 LDA n'est pas exhaustive). Mais en tout cas, le site ne peut pas être assimilé à un programme d'ordinateur au sens de l'art. 2 al. 3 LDA.

Un autre argument invoqué par la doctrine contre cette assimilation est qu'un logiciel doit pouvoir être exécuté de manière autonome ; or, un site web n'a pas cette qualité, puisqu'il faut disposer d'un navigateur Internet (browser) pour pouvoir le consulter[10].

C. Le site Internet en tant qu'œuvre dérivée ou recueil

Lorsque des œuvres artistiques préexistantes (par exemple des vidéos) sont intégrées dans le site, la protection conférée à celles-ci est réservée d'après l'art. 3 al. 4 LDA. Par conséquent, si ces œuvres sont reproduites à des fins privées, le fait que le site contienne des logiciels non soumis à l'exception d'usage privé[11] ne doit pas affecter les rémunérations dues sur la base de l'art. 20 LDA en faveur desdites œuvres artistiques préexistantes. La même conclusion s'imposerait si l'on devait qualifier le site de recueil au sens de l'art. 4 LDA[12]. Parallèlement, le site lui-même est protégé en tant que création dérivée s'il a un caractère individuel[13]. Cette création dérivée est donc une « autre œuvre visuelle ou audiovisuelle » ou une œuvre multimédia *sui generis*[14]. Rien ne permet d'affirmer que le régime juridique spécifique applicable aux logiciels soit valable pour cette œuvre dérivée. En effet, comme indiqué ci-dessus, celle-ci n'est pas uniquement un logiciel, c'est-à-dire une succession d'ordres destinés à l'ordinateur. Or, les règles légales

5 *Ibidem*.
6 BUEHLER, p. 127-129.
7 GILLIÉRON, p. 260 ; BUEHLER, p. 124 ; RENOLD, p. 94 ; CHERPILLOD, SHK, N 61 ad art. 2 LDA.
8 Dans ce sens : BARRELET/EGLOFF, N 19 et 20 ad art. 2 LDA.
9 Dans ce sens, voir BUEHLER, p. 131-132.
10 GILLIÉRON, p. 261 ; BUEHLER, p. 127.
11 Art. 19 al. 4 LDA.
12 Cf. art. 4 al. 2 LDA ; sur ces questions, voir Message du CF, FF 1993 III 511.
13 Art. 3 al. 1 ou art. 4 al. 1 LDA.
14 Voir *supra* I.B.

concernant les logiciels sont des normes d'exception[15]. Pour les autres œuvres, parmi lesquelles figurera l'œuvre dérivée, les règles ordinaires de la LDA seront applicables.

D. Le site Internet en tant qu'œuvre collective

Lorsque les différents apports (textes, graphisme, images, musique, séquences de films, etc.) sont créés spécialement pour le site Internet par plusieurs personnes, il faut se demander dans quelle mesure l'art. 7 LDA est applicable. D'après cette disposition, les coauteurs seraient titulaires en commun d'un seul droit d'auteur sur le site[16]. A propos de la musique des pièces de théâtre, le Tribunal fédéral a eu l'occasion de préciser que « *selbst wenn jedoch eine Musikeinrichtung speziell im Hinblick auf ein Schauspiel komponiert wird, liegt in aller Regel keine Miturheberschaft und damit keine Gesamthand im Sinne von Art. 7 URG vor. Dies wäre nur anzunehmen, wenn Komponist und Autor in beiderseitigem Zusammenwirken das Schauspiel gemeinsam erarbeiten* »[17]. L'art. 7 LDA s'applique donc si les coauteurs créent l'œuvre en concourant réciproquement, de sorte qu'ils cordonnent les différents apports les uns par rapport aux autres, en les destinant et en les subordonnant à une œuvre collective[18]. En d'autres termes, il faut que chaque auteur tienne compte de la création des autres pour parfaire la sienne.

Dans le cas – imaginable mais plutôt rare – où un logiciel est créé spécialement pour un site Internet, on doit douter qu'il y ait un « concours réciproque » entre l'auteur du logiciel et les auteurs des œuvres « artistiques » comme le graphisme, les textes, la musique, etc. L'auteur du logiciel tiendra certes compte des œuvres artistiques puisque son programme devra les faire « fonctionner ». En revanche, le graphiste, l'auteur des textes ou le compositeur créeront leurs contributions sans se préoccuper du logiciel. Cela déjà, parce qu'ils n'auront souvent pas les connaissances techniques nécessaires. De son côté, l'auteur du logiciel travaillera seul, sur la base des apports fournis par les autres créateurs, mais il n'influencera normalement pas ces apports (également parce qu'un informaticien n'est pas nécessairement un graphiste, un rédacteur ou un compositeur). Dans un tel cas, il n'y aura donc pas de droit d'auteur commun, mais chaque type d'apport (logiciel et autres créations) fera l'objet d'une protection séparée. Il en découle notamment que les art. 19 et 20 LDA s'appliqueront à toutes les autres créations que le logiciel.

---

15 BUEHLER, p. 128.

16 Art. 7 al. 1 LDA.

17 TF 2A_180/1994 du 10 mai 1995 (non publié), consid. 3f aa, dans la cause Schweizerischer Bühnenverband et consorts c./ SUISA et Commission arbitrale fédérale pour la gestion de droits d'auteur et de droits voisins.

18 Voir TF 2A_288/2002 du 24 mars 2003, consid. 3.4.2, in : sic ! 9/2003, p. 699 ss, « Tarif VN ».

Un concours réciproque au sens de la jurisprudence précitée est surtout envisageable lorsque plusieurs personnes participent à la création d'un apport relevant du même genre, par exemple si deux personnes réalisent ensemble le texte d'une page Internet[19]. Dans ce cas, le droit d'auteur sur l'apport leur appartiendra en commun[20] ; ils ne pourront en disposer que d'un commun accord, étant précisé qu'aucun d'eux ne pourra refuser son accord pour des motifs contraires aux règles de la bonne foi[21].

II. L'acquisition des droits sur les œuvres préexistantes

A. Introduction

Lorsqu'un travailleur crée un site web, une page Facebook, etc. pour le compte de son employeur, il est fréquemment amené à utiliser des œuvres préexistantes (logiciels, photos, etc.). Se pose donc la question de l'acquisition des droits sur ces créations. Une utilisation de ces dernières sans les autorisations nécessaires représenterait un acte illicite au sens des art. 41 ss CO[22]. A cet égard, l'employeur répond des actes de ses employés, conformément aux principes de la responsabilité causale prévue par l'art. 55 CO. Pour lui, il est donc particulièrement important que les travailleurs acquièrent de manière régulière les différents droits nécessaires. Il aura notamment le devoir de les instruire et de les surveiller dans le processus d'obtention des licences. D'où l'importance pour lui de maîtriser le sujet.

B. Les droits mis en jeu

Comme son nom l'indique, la Loi sur le droit d'auteur instaure avant tout des droits en faveur des auteurs d'œuvres littéraires et artistiques (auxquelles les logiciels sont assimilés[23]), c'est-à-dire des personnes qui les ont créées. Elle leur confère deux types de prérogatives : les droits moraux et les droits patrimoniaux[24]. Les premiers regroupent le

19 L'application de l'art. 7 LDA en cas de création par plusieurs personnes d'apports relevant de genres différents (par exemple le graphisme et des photographies) n'est pas exclue en soi, mais devrait être plus rare en pratique.
20 Art. 7 al. 1 LDA.
21 Art. 7 al. 2 LDA.
22 Cf. art. 62 al. 2 LDA.
23 Art. 2 al. 3 LDA.
24 BARRELET/EGLOFF, N 3 ad art. 9 LDA.

droit de revendiquer la paternité de son œuvre[25], celui de décider de sa divulgation[26] et celui de s'opposer aux atteintes à son intégrité, notamment lorsqu'elle est utilisée pour créer une œuvre dérivée ou un recueil[27]. Les droits moraux visent à préserver le lien particulier qui unit l'auteur à son œuvre. Quant aux droits patrimoniaux, ils ont plutôt pour fonction de permettre à l'auteur d'obtenir une rémunération grâce à sa création : l'art. 10 LDA dispose de manière générale que l'auteur a le droit exclusif de décider si, quand et de quelle manière son œuvre sera utilisée. A titre exemplatif, l'article énumère ensuite un certain nombre de prérogatives : l'auteur a en particulier le droit de confectionner des exemplaires de son œuvre[28], de proposer ces exemplaires au public[29], de réciter, représenter ou exécuter son œuvre[30], etc. Vu que la loi confère ainsi un monopole à l'auteur sur sa création, le premier a le pouvoir de s'opposer à l'utilisation de la seconde ou de l'autoriser à certaines conditions, par exemple celle d'être rémunéré. Le monopole est la règle. Cependant, la loi prévoit aussi différentes exceptions ou restrictions au droit d'auteur[31], par exemple pour l'usage privé[32], pour les citations[33] ou pour les comptes rendus d'actualité[34].

En cas de création et d'exploitation d'un site web contenant des œuvres préexistantes, deux droits patrimoniaux sont touchés. Tout d'abord, le droit de reproduire ces œuvres préexistantes, puisque leur introduction dans une mémoire informatique est une reproduction au sens de l'art. 10 al. 2 let. a LDA[35]. De plus, l'acte de « *uploading* » sera aussi, simultanément, une mise à disposition permettant à chacun d'avoir accès à l'œuvre « *de l'endroit et au moment qu'il choisit individuellement* ». Le droit de l'art. 10 al. 2 let. c LDA sera donc aussi en jeu[36]. En ce qui concerne les droits moraux, le droit à l'intégrité de l'art. 11 LDA pourra être concerné, puisque l'œuvre préexistante sera utilisée pour la création de l'œuvre dérivée (ou du recueil) que constituera en principe le site web[37]. Dans le domaine de la musique, lorsqu'une composition est intégrée dans une œuvre audiovisuelle ou multimédia, le droit à l'intégrité concerné est appelé « droit de synchronisation ».

25 Art. 9 al. 1 LDA.
26 Art. 9 al. 2 LDA.
27 Art. 11 LDA.
28 Art. 10 al. 2 let. a LDA.
29 Art. 10 al. 2 let. b LDA.
30 Art. 10 al. 2 let. c LDA.
31 Voir notamment le chapitre 5 LDA.
32 Art. 19 LDA.
33 Art. 25 LDA.
34 Art. 28 LDA.
35 BARRELET/EGLOFF, N 12 ad art. 10 LDA ; GILLIÉRON, p. 271.
36 BARRELET/EGLOFF, N 12, 22 et 22a ad art. 10 LDA.
37 Art. 11 al. 1 let. b LDA.

En outre, la loi sur le droit d'auteur ne protège pas que les créateurs : elle confère aussi des droits dits « voisins » aux artistes interprètes, aux producteurs de phonogrammes et de vidéogrammes, de même qu'aux organismes de diffusion (radios et télévisions)[38]. Ces personnes physiques ou morales bénéficient de droits patrimoniaux semblables à ceux des auteurs. En particulier, elles disposent du droit exclusif de reproduire leurs prestations, respectivement leurs enregistrements et émissions[39], de même que du droit de les mettre à disposition sur un réseau comme Internet[40]. En outre, les artistes interprètes bénéficient de droits moraux sur leurs prestations, qui leur permettent de faire reconnaître leur qualité d'artistes interprètes, et de s'opposer aux altérations de leurs prestations sur la base des art. 28 à 28*l* du CC[41].

C. L'acquisition des droits sur les logiciels

Schématiquement, on peut distinguer deux types de logiciels relatifs aux sites Internet. Il y a tout d'abord les « serveurs web »[42] (*Webserversoftware*) ou serveurs HTTP, qui sont en quelques sortes les outils permettant aux sites de fonctionner[43]. Il y a ensuite les systèmes de gestion de contenu (*Content Management System*, CMS), qui sont des logiciels destinés à la conception et à la mise à jour du contenu figurant sur un site[44]. Les conditions de licence varient d'un logiciel à l'autre, mais elles sont généralement clairement expliquées à l'utilisateur. On trouve des licences de type « propriétaire » aussi bien que des licences dites « libres ». Dans le domaine des logiciels, une licence est dite propriétaire ou privative si les conditions d'utilisation qu'elle définit entravent l'un des droits donnés par les licences libres, à savoir *utiliser*, *étudier*, *modifier*, *dupliquer* ou *diffuser* l'œuvre sur laquelle porte la licence[45]. Les licences propriétaires imposent fréquemment à l'utilisateur le paiement d'une redevance. Toutefois, un logiciel serveur HTTP, comme Microsoft IIS, est déjà intégré dans les serveurs basés sur le système d'exploitation Windows (version professionnelle)[46], quand bien même il fait l'objet d'une licence propriétaire. Le plus connu des logiciels « serveurs web » est certainement

38 Art. 33 ss LDA.
39 Art. 33 al. 2 let. c, 36 let. a et 37 let. c LDA.
40 Art. 33 al. 2 let. a, 36 let. b et 37 let. e LDA.
41 Art. 33a LDA.
42 Cette expression désigne aussi bien le matériel (c'est-à-dire l'ordinateur) que le logiciel.
43 Ils servent des requêtes respectant le protocole HTTP : voir http://fr.wikipedia.org/wiki/Serveur_web (consulté le 1er novembre 2013).
44 Voir : http://fr.wikipedia.org/wiki/Syst%C3%A8me_de_gestion_de_contenu (consulté le 1er novembre 2013).
45 http://fr.wikipedia.org/wiki/Licence_propri%C3%A9taire (consulté le 1er novembre 2013).
46 http://fr.wikipedia.org/wiki/Internet_Information_Services (consulté le 1er novembre 2013).

Apache[47], qui est disponible sous licence libre[48] de type « open source »[49]. Quant aux CMS, on signalera l'existence de Joomla ![50] et de Typo 3[51], qui sont tous deux des logiciels libres publiés sous la licence publique générale GNU[52]. Ils sont disponibles gratuitement.

En résumé, l'acquisition des droits sur les logiciels ne devrait pas être problématique pour une entreprise, ni juridiquement ni financièrement.

D. L'acquisition des droits sur les œuvres littéraires et artistiques préexistantes

1. Le contact des ayants droit individuellement

En revanche, l'acquisition des droits sur les œuvres littéraires et artistiques préexistantes sera souvent plus compliquée. Fondamentalement, il faudra contacter tous les ayants droit. Cependant, ceux-ci seront fréquemment difficiles à identifier, on ne connaîtra pas leurs coordonnées ou alors ... ils ne répondront pas ! Deux moyens existent toutefois pour simplifier le processus de régularisation des droits : la gestion collective et les licences libres ou de libre diffusion.

2. La gestion collective

Les organismes de gestion collective sont des sociétés qui exercent leur activité à titre fiduciaire : il s'agit de personnes morales, sans but lucratif[53], auxquelles les auteurs et autres ayants droit confient le soin de faire valoir les droits patrimoniaux auprès des exploitants. Leurs membres sont des créateurs, c'est-à-dire des compositeurs, des parolliers, des écrivains, des réalisateurs, etc., ou des titulaires de droits à titre dérivé comme des producteurs ou des éditeurs. Elles représentent des milliers d'ayants droit et agissent pour eux comme « guichet unique » habilités à délivrer des licences pour le compte de tous.

---

47 http://fr.wikipedia.org/wiki/Apache_HTTP_Server (consulté le 1er novembre 2013).

48 http://fr.wikipedia.org/wiki/Licence_Apache (consulté le 1er novembre 2013).

49 http://fr.wikipedia.org/wiki/Open_source (consulté le 1er novembre 2013).

50 http://fr.wikipedia.org/wiki/Joomla! (consulté le 1er novembre 2013).

51 http://fr.wikipedia.org/wiki/TYPO3 (consulté le 1er novembre 2013).

52 http://fr.wikipedia.org/wiki/Licence_publique_g%C3%A9n%C3%A9rale_GNU (consulté le 1er novembre 2013).

53 En Suisse, les sociétés de gestion sont légalement tenues de ne pas viser de but lucratif : art. 45 al. 3 LDA.

En Suisse, il existe actuellement cinq organismes de gestion collective : ProLitteris pour l'art littéraire et plastique, la Société Suisse des Auteurs (SSA) pour les œuvres dramatiques, dramatico-musicales, chorégraphiques et pour certaines œuvres audiovisuelles ou multimédia, SUISA pour les œuvres musicales non théâtrales, Suissimage pour les créations audiovisuelles et enfin Swissperform, pour les droits à rémunération instaurés dans le domaine des droits voisins. Les quatre premières (ProLitteris, la SSA, SUISA et Suissimage) sont des coopératives[54], alors que Swissperform a la forme juridique d'une association[55].

Dans certains domaines, les ayants droit sont tenus de recourir aux sociétés de gestion collective pour faire valoir leurs droits[56]. Toutefois, cela ne vaut normalement pas pour les droits mis en jeu par la création et l'exploitation d'un site Internet. En ce domaine, la gestion collective n'est que facultative pour les ayants droit, si bien que la représentativité des sociétés de gestion collective varie. Par exemple, pour les arts visuels et la photographie, ProLitteris gère le droit de reproduction[57] ; de même, elle exerce le droit de mise à disposition à la demande[58] des textes, ainsi que des œuvres d'art visuel et photographiques. Il existe un portail OLA (On line Art), par l'intermédiaire duquel ProLitteris fait valoir les droits de ses propres membres et, basée sur des contrats avec des sociétés-sœurs, également d'ayants droit étrangers, c'est-à-dire au total d'environ 40'000 auteurs d'art figuratifs[59]. Les droits de mise à disposition et de reproduction sont aussi gérés par la SSA au profit des auteurs, s'agissant de son répertoire audiovisuel et scénique. Suissimage exerce le droit de reproduire des extraits d'œuvres audiovisuelles, mais cela uniquement dans des produits multimédias « off line » (donc pas dans des sites Internet)[60]. Quant à SUISA, elle est active dans tout le domaine de la reproduction et de la mise à disposition en ligne d'œuvres musicales non théâtrales[61]. Environ la moitié du répertoire mondial de musique est ainsi géré en Suisse par SUISA, s'agissant de la distribution à la demande par Internet. Pour ses propres membres, SUISA est aussi

54 Au sens des art. 828 ss CO.

55 Au sens des art. 60 ss CC.

56 Voir par exemple : art. 13 al. 3, art. 20 al. 4, art. 22, art. 22*a* à 22*c* LDA, etc.

57 Art. 10 al. 2 let. a LDA.

58 Art. 10 al. 2 let. c *in fine* LDA.

59 Voir www.onlineart.info (consulté le 1er novembre 2013).

60 Voir http://www.suissimage.ch/fileadmin/content/pdf/3_Nutzer_Tarife/offlinef.pdf (consulté le 1er novembre 2013).

61 En ce domaine, elle n'est d'ailleurs pas surveillée par la Confédération, le droit de mise à disposition n'étant pas mentionné par l'art. 40 al. 1 let. a LDA, pas plus que le droit de reproduction sur des serveurs informatiques.

présente à l'étranger et elle délivre des licences « multi-territoriales » pour les utilisations en ligne, cela depuis l'automne 2013[62].

Il faut cependant savoir que les sociétés de gestion collective ne seront pas toujours habilitées à accorder des autorisations au titre du droit moral ou des droits voisins. La régularisation des droits d'auteur patrimoniaux par leur intermédiaire n'est donc pas toujours suffisante. Notamment, il en va ainsi dans le domaine musical : l'autorisation de SUISA ne dispense normalement pas l'utilisateur de contacter l'éditeur de l'œuvre pour obtenir le droit de synchronisation (droit à l'intégrité), de même que le producteur de l'enregistrement pour obtenir les droits voisins[63]. Il existe cependant des catalogues musicaux spécialement offerts en vue de la sonorisation de produits audiovisuels ou multimédia. On parle alors de « *mood music* ». Pour celle-ci, le droit de synchronisation et les droits voisins sont également confiés à SUISA, pour qu'elle puisse accorder une autorisation globale, couvrant tous les droits. Dans la mesure du possible, il est fortement conseillé d'utiliser ces catalogues de « *mood music* » en cas de sonorisation d'un site web, puisque le processus de régularisation des droits en sera très simplifié.

3. Les licences libres et de libre diffusion

Une licence est un contrat par lequel le titulaire des droits d'auteur autorise certaines utilisations de l'œuvre. Une licence « libre », au sens large du terme, est une déclaration publique, souvent donnée par Internet, par laquelle le titulaire des droits autorise à l'avance toute personne à accomplir certaines utilisations de l'œuvre[64]. Au sens étroit, une licence libre sur une œuvre littéraire et artistique confère les quatre possibilités suivantes[65] :

- utiliser l'œuvre, pour tous les usages ;
- étudier l'œuvre ;
- redistribuer des copies de l'œuvre ;
- modifier l'œuvre et publier ces modifications.

---

62 Voir SUISAinfo 2.13, p. 12.

63 Le producteur sera habilité à traiter les droits voisins dont il bénéficie originairement d'après l'art. 36 LDA, de même que les droits voisins de l'artiste interprète selon l'art. 33 LDA qu'il aura acquis par cession contractuelle (le producteur se fait normalement céder les droits de l'artiste interprète par le contrat de production qu'il passe avec ce dernier).

64 On peut difficilement parler de contrat, puisque les conditions d'utilisation ne sont pas expressément acceptées par l'utilisateur.

65 http://fr.wikipedia.org/wiki/Licence_libre (consulté le 1er novembre 2013).

La licence est dite « de libre diffusion » si la déclaration publique confère seulement certaines des libertés susmentionnées[66]. En revanche, elle est « libre » si les quatre libertés sont accordées en totalité. La licence libre est donc animée par une volonté éthique d'égalité, ce qui ne vaut pas forcément pour la licence de libre diffusion.

Les licences Creative Commons sont un exemple de licences libres ou de libre diffusion. Elles contiennent des clauses juridiques complètes et détaillées, dont l'essentiel est résumé par des pictogrammes[67]. Ceux-ci apparaissent au moment de la consultation de l'œuvre (notamment sur Internet), avec un renvoi au texte complet des conditions[68].

On trouve ainsi sur Internet des œuvres sous licences Creative Commons (par exemple des photographies ou des textes), que l'on pourra utiliser dans le cadre d'un site web, à condition de respecter les conditions imposées par la licence[69]. Les licences Creative Commons sont concédées à titre gratuit. Là aussi, l'acquisition des droits sera donc grandement facilitée.

III. L'acquisition des droits sur le site ou sur le compte

A. Introduction

Parmi les problèmes générés par l'utilisation des médias sociaux comme outils de communication d'une entreprise, se pose celui de savoir à qui confier la tâche de créer et de gérer la plateforme choisie (responsable du département de communication, employé, « *community manager* » ?). En fonction des choix réalisés, viendra vite la question de savoir à qui appartient le compte[70] et qui est titulaire des éventuels droits d'auteur s'y rapportant.

Même si le site ou le blog considéré a été développé par des travailleurs dans l'exercice de leur activité au service de l'employeur, la solution sera différente suivant que c'est son aspect « artistique » (graphisme, image, texte et musique) ou logiciel qui est envisagé.

---

66 http://fr.wikipedia.org/wiki/Licence_de_libre_diffusion (consulté le 1er novembre 2013). Dans le domaine des logiciels, on parlera déjà de licence « propriétaire » si les quatre libertés caractérisant une licence libre ne sont pas réunies en totalité.

67 Voir http://fr.wikipedia.org/wiki/Creative_Commons (consulté le 1er novembre 2013).

68 Les textes de l'encyclopédie wikipédia sont publiés sous licences creative commons : www.wikipedia.org.

69 Souvent, la seule condition sera de citer le nom de l'auteur.

70 Dans ce sens, ROBERT ; voir aussi concernant l'assimilation des blogs aux sites web, TF 5A_792/2011 du 14 janvier 2013, consid. 6.1 et réf. citées.

Quant à la question des droits voisins du droit d'auteur, elle ne se pose que dans l'hypothèse, somme toute peu vraisemblable, où les salariés ayant participé à la création d'une plateforme de médias sociaux pour leurs employeurs auraient interprété eux-mêmes les œuvres de celle-ci, par exemple la musique, plutôt que de profiter des catalogues de « *mood music* » pour la sonoriser[71].

Dans la mesure enfin où la réalisation de la plateforme ou du compte serait confiée à un tiers externe à l'entreprise qui se destine à l'exploiter, ce sont les dispositions du mandat ou du contrat d'entreprise qui auront vocation à s'appliquer[72].

B. Le développement de la plateforme par des employés

Il est encore assez communément répandu de croire à tort que les droits d'auteur appartiennent automatiquement à l'employeur lorsqu'on est en présence d'œuvres protégées par le droit d'auteur créées par des auteurs salariés dans le cadre d'un rapport de travail[73]. En effet, sauf pour ce qui est des droits sur les logiciels développés par des travailleurs dans l'exercice de leur activité au service de l'employeur et conformément à leurs obligations contractuelles (art. 17 LDA), ni la loi sur le droit d'auteur, ni le Code des obligations[74], ne régissent spécifiquement le statut des œuvres réalisées par des auteurs employés[75]. Il est en outre admis que l'art. 332 CO, qui concerne les inventions et les designs de travailleurs, ne s'applique pas par analogie aux œuvres de salariés[76]. C'est donc à la convention qui lie l'auteur à son employeur (qu'il s'agisse d'un contrat individuel de travail ou d'une convention collective[77]) qu'il revient de régler la titularité des droits d'auteur sur les créations intervenues dans le cadre des rapports de travail.

---

71 Voir *supra* II.D.2 *in fine*.

72 Voir *infra* III.C.

73 Dont on constate d'ailleurs qu'elles sont de plus en plus nombreuses aujourd'hui, voir ALDER, p. 463.

74 Qui ne comporte pas de disposition expresse qui soit pour les droits d'auteur le pendant de l'art. 332 CO pour les brevets et les designs, voir dans ce sens ALDER, p. 476 et DE WERRA, SHK, N 43 ad art. 16 LDA.

75 WYLER, p. 383 et ANDERMATT, p. 293.

76 Voir SEILER, p. 102 et réf. citées, en particulier ATF 74 II 106, consid. 4a ; voir aussi DE WERRA, CR-PI, N 2 ad art. 17 LDA et BARRELET/EGLOFF, N 1 ad art. 17 LDA, quant au fait que même pour les logiciels développés par les travailleurs, le Parlement n'a pas souhaité renvoyer à l'art. 332 al. 1 CO et a préféré la solution de l'art. 17 LDA.

77 Voir dans ce sens ALDER, p. 476, WYLER, p. 383 et réf. citées et DE WERRA, CR-PI, N 5 ad art. 16 LDA.

1. Le principe du créateur

A défaut de disposition spécifique dans le Code des obligations et dans la LDA concernant la titularité des droits d'auteur sur les œuvres, autres que les logiciels, créées par des salariés, il convient d'appliquer les règles de base de la LDA, dont le principe du créateur. Ce principe découle de l'art. 6 LDA qui prévoit que l'auteur est la personne physique qui a créé l'œuvre. Il s'agit d'une « des maximes fondamentales de la législation suisse en matière de droit d'auteur »[78] bénéficiant de la garantie constitutionnelle de la propriété, au même titre que l'ensemble des principes de base du droit de la propriété intellectuelle. Il ne peut ainsi valablement y être dérogé que conventionnellement ou par une base légale claire, comme l'art. 332 CO pour les inventions et les designs[79], ou comme l'art. 17 LDA pour les logiciels de service[80]. Ce principe s'applique aussi aux œuvres créées sur commande ou par des salariés[81] et la titularité des droits d'auteur revient alors à l'employé faute de disposition contractuelle contraire. L'employeur ne peut en devenir propriétaire qu'à titre dérivé[82]. Pour qu'un transfert des droits d'auteur de l'employé à son employeur entre en ligne de compte, il faut soit que le contrat de travail (ou la convention collective[83]) le prévoie expressément, soit qu'il découle de manière implicite du contrat, en particulier du but poursuivi par les parties en contractant, en application de la théorie de la finalité[84].

2. Les logiciels de service, art. 17 LDA

Comme il a été exposé plus haut[85], un site Internet ne peut pas être assimilé à un programme d'ordinateur au sens de l'art. 2 al. 3 LDA. Même si sa réalisation a été confiée à des travailleurs et est intervenue dans le cadre de leur activité au service de l'employeur et conformément à leurs obligations contractuelles, les droits exclusifs

78 ATF 116 II 351, JdT 1991 I 616 (rés.), VereinG, cité par BARRELET/EGLOFF, N 1 ad art. 6 LDA.

79 Voir dans ce sens ANDERMATT, p. 286.

80 DE WERRA, CR-PI, N 1 ad art. 17 LDA, qui précise que l'art. 17 LDA, sans constituer une exception au principe du créateur « attribue toutefois à l'employeur le droit exclusif d'utilisation sur des logiciels créés par des employés » ; voir aussi ALDER, p. 475.

81 CHERPILLOD, CR-PI, N 6 ad art. 6 LDA.

82 ANDERMATT, p. 290 ; CHERPILLOD CR-PI, N 5 ad art. 6 LDA.

83 ALDER, p. 496, relève que lorsqu'une cession du droit d'auteur est prévue par une convention collective elle peut être assimilée vu l'effet « normatif » des conventions collectives découlant de l'art. 357 al. 1 CO « à une cession légale des droits d'utilisation ».

84 Voir *infra* III.B.3.

85 Voir *supra* I.B.

d'utilisation portant sur ce site dans son ensemble ne sauraient être exercés exclusivement par l'employeur en vertu de l'art. 17 LDA[86].

Qu'un site soit une œuvre dérivée multimédia, un recueil ou une œuvre collective, il convient de considérer que chacun des éléments du site (graphisme, texte, musique, support logiciel) jouira d'une protection séparée[87]. L'employeur pourra ainsi bénéficier d'une autorisation d'exercer les droits exclusifs d'utilisation sur les parties logicielles du site qui sera, le cas échéant, indépendante de l'acquisition des droits d'auteur portant sur les autres aspects de l'œuvre.

L'application de l'art. 17 LDA aux éléments logiciels d'un site ou d'un compte Internet suppose qu'ils soient protégés par le droit d'auteur[88] et qu'ils aient été créés dans le cadre d'un rapport de travail[89], par le travailleur ayant ainsi agi « au service de l'employeur et conformément à ses obligations contractuelles »[90]. Cela implique que la réalisation de ces parties logicielles soit intervenue en exécution des obligations contractuelles du travailleur[91], lesquelles peuvent être déterminées par analogie avec les principes posés par la doctrine et la jurisprudence concernant les obligations contractuelles du travailleur auteur d'un design ou d'une invention selon l'art. 332 CO[92]. Le lieu et le moment de la réalisation du logiciel, pour autant que celle-ci soit intervenue avant la fin des rapports de travail[93], comptent peu.

---

86 Voir *supra* I.C sur le caractère particulier des dispositions sur les logiciels qui sont des normes d'exception s'appliquant aux logiciels uniquement.

87 Voir *supra* I.D.

88 DE WERRA, CR-PI, N 6 ad art. 17 LDA, qui souligne que l'employé sera tenu de remettre à son employeur les autres prestations qui peuvent lui profiter, mais ne sont pas protégées par le droit d'auteur, en vertu de l'art. 321*b* al. 2 CO. On pourrait ainsi penser aux codes d'accès par exemple ; voir dans le même sens et pour les résultats du travail qui échappent à la réglementation particulière de l'art. 332 CO, TISSOT, CR-PI, N 33 ad art. 3 LBI et réf. citées ; WYLER, p. 384, précise que « le recours aux devoirs de diligence et de fidélité, ainsi qu'à l'obligation de rendre compte et de restituer n'est admissible qu'en l'absence de législation spéciale traitant la question de l'appartenance des droits de propriété intellectuelle sur les créations considérées [art. 332 CO, 9 LPOV et 17 LDA] ».

89 BARRELET/EGLOFF, N 3 ad art. 17 LDA et DE WERRA, CR-PI, N 8 ad art. 17 LDA, relèvent que « l'art. 17 LDA n'est pas applicable à des programmes créés par des personnes hors d'un contrat de travail », par exemple par des développeurs de logiciels indépendants (voir *infra* III.C) ou dans le cadre de relations de droit public.

90 BARRELET/EGLOFF, N 4 ad art. 17 LDA.

91 BARRELET/EGLOFF, N 4 ad art. 17 LDA

92 Voir pour un examen des conditions qui doivent être remplies, TISSOT, Commentaire, N 4 et N 10 ad art. 332 CO.

93 ALDER, p. 484, qui relève (traduction libre) que « l'employé qui quitte l'entreprise n'a pas le droit d'emporter avec lui ou de détruire les œuvres de service ou les parties de celles-ci déjà commencées avant l'échéance des rapports de travail » ; voir aussi BARRELET/EGLOFF, N 5 ad art. 17 LDA, qui

A la différence de ce qui se produit dans le cadre de l'art. 332 CO pour les designs et les inventions de service, l'employeur ne sera pas investi des droits d'utilisation sur les logiciels créés par ses travailleurs dans l'exercice de leur activité au service de l'entreprise et conformément à leurs obligations contractuelles, mais seulement autorisé à les exercer de manière exclusive[94]. Les droits d'utilisation, dont l'exercice revient ainsi de manière exclusive à l'employeur, comportent aussi les droits de modification et d'adaptation[95].

Pour les logiciels qui ne remplissent pas les conditions de l'art. 17 LDA, ne peuvent donc pas être qualifiés de « logiciels de service »[96], et à propos desquels le contrat de travail (ou la convention collective) ne prévoirait pas une acquisition à titre dérivé des droits d'auteur par l'employeur[97], ce sont les principes qui président habituellement au transfert

précisent que si le logiciel n'est terminé qu'après la fin des rapports de travail, l'art. 17 LDA ne peut concerner que les parties et projets présentant un caractère individuel suffisant pour être protégé par le droit d'auteur déjà élaborés au moment de la fin du contrat. Les logiciels dont l'achèvement auraient été, à dessein, repoussé après l'échéance du contrat de travail devraient, par analogie avec ce qui se fait pour les designs et les inventions de service, être réputés réalisés pendant le contrat. Voir pour les inventions et les designs, TISSOT, Commentaire, N 4 ad art. 332 CO et réf. citées.

94 Voir BARRELET/EGLOFF, N 6 ad art. 17 LDA et réf. citées, pour l'illustration de la controverse doctrinale sur la question de savoir si l'art. 17 LDA constitue une licence ou une cession légale des droits d'utilisation. Du moment toutefois que cette licence est exclusive et que l'employeur est dès lors au bénéfice de la qualité pour agir contre des tiers (art. 62 al. 3 et 65 al. 5 LDA), sa situation n'est matériellement pas bien différente de celle qui serait la sienne s'il était propriétaire des droits concernés. C'est surtout en relation avec la possibilité pour l'employeur de disposer à son tour des droits d'auteur, ainsi qu'en lien avec la résiliation du contrat ou dans le cadre d'une faillite éventuelle, que la différence entre une cession et une licence légale conserve une certaine portée. Voir dans ce sens ALDER, p. 489 et aussi DE WERRA, SHK, N 7 ad art. 16 LDA. Le fait que le législateur ait expressément exclu l'application de l'art. 332 aux logiciels de service (voir note 76 ci-dessus) paraît aussi militer en faveur de l'institution d'une licence légale plutôt que d'une cession ; voir toutefois contra, en particulier, DE WERRA, CR-PI, N 17 ad art. 17 LDA, qui recommande néanmoins (N 14 ad art. 17 LDA) « dans l'intérêt de l'employeur d'adapter une réglementation contractuelle visant à clarifier que la création de logiciels fait partie intégrante des activités couvertes par les obligations contractuelles du travailleur » en relevant que si le contrat de travail prévoit « une cession de tous les droits d'auteur sur les logiciels créés par le travailleur dans le cadre de ses obligations de service » cela exclut l'application de l'art. 17 LDA.

95 BARRELET/EGLOFF, N 7 ad art. 17 LDA ; DE WERRA, CR-PI, N 20 ad art. 17 LDA ; ALDER, p. 493.

96 La tentation de parler de « logiciels de service » pour les créations dont la réalisation satisfait aux conditions de l'art. 17 LDA est grande vu le parallèle possible avec les conditions d'application de l'art. 332 CO. Il ne se justifie toutefois pas de qualifier ensuite les logiciels dont la création n'est pas intervenue dans le cadre des obligations contractuelles de leur auteur au sens de l'art. 17 LDA de « logiciels occasionnels ou réservés » ou de « logiciels libres » puisque l'analogie avec l'art. 332 CO ne saurait valoir pour ces types de réalisations qui sont soumises aux règles générales de l'art. 16 LDA ; voir dans ce sens BARRELET/EGLOFF, N 4 ad art. 17 LDA.

97 DE WERRA, CR-PI, N 3 ad art. 17 LDA ; voir aussi SEILER, p. 102.

du droit d'auteur qui doivent être appliqués[98]. Il convient donc de rechercher si les parties ont envisagé et voulu un transfert des droits d'auteur du créateur à son employeur et quelle est, le cas échéant, la portée de la cession convenue[99].

Finalement, il importe de relever qu'« à défaut d'une élection de droit, les contrats de travail sont soumis au droit de l'Etat dans lequel l'employé exerce habituellement son activité professionnelle »[100]. Par conséquent et par défaut, l'art. 17 LDA s'applique aux contrats de travail qui se rapportent aux développements de logiciels ayant lieu dans notre pays et doit être compris comme une licence (respectivement une cession) légale sans limitation géographique ne valant pas seulement pour les « droits d'auteur suisses » liés à ces réalisations[101]. Pareillement, la licence ou la cession légale instituée par l'art. 17 LDA en faveur de l'employeur ne vaut pas seulement pour les droits d'utilisation connus au moment de l'achèvement du développement, mais aussi pour les droits d'utilisations futures encore inconnus à ce moment-là[102].

3. L'acquisition à titre dérivé des droits par l'employeur pour les autres catégories d'œuvres

« En vertu de l'art. 16 al. 1 LDA, les droits d'auteur sont cessibles. Ainsi, tous les droits d'utilisation énumérés à l'art. 10 al. 2 LDA peuvent être cédés individuellement ou de façon globale à des tiers »[103], et notamment à l'employeur des auteurs salariés à l'origine des créations graphiques, littéraires, musicales ou multimédias, qui constituent le site ou le compte web à la réalisation duquel ils ont participé. « Le transfert du droit d'auteur peut avoir une portée très variable »[104] ; n'est pas soumis à une exigence de forme particulière[105] ; peut intervenir sur la base de différents types de contrats dont le contrat de travail notamment[106] ; et ne suppose même pas que « l'auteur ait la connaissance de l'existence et de l'étendue des droits qu'il cède sur son œuvre »[107]. Le fait qu'il subodore l'existence de tels droits, et qu'il renonce à les faire valoir à l'encontre de leurs

98 BARRELET/EGLOFF, N 4 ad art. 17 LDA.
99 Voir *infra* III.B.3.
100 DE WERRA, CR-PI, N 5 ad art. 17 LDA ; voir dans le même sens pour les inventions et designs des travailleurs, TISSOT, CR-PI, N 32 ad art. 3 LBI et réf. citées.
101 Voir dans ce sens, DE WERRA, CR-PI, N 5 ad art. 17 LDA.
102 DE WERRA, CR-PI, N 27 ad art. 17 LDA.
103 DE WERRA, CR-PI, N 6 ad art. 16 LDA et DE WERRA, SHK, N 6 ad art. 16 LDA.
104 BARRELET/EGLOFF, N 2 ad art. 16 LDA.
105 BARRELET/EGLOFF, N 3b ad art. 16 LDA, DE WERRA, CR-PI, N 34 ad art. 16 LDA et DE WERRA, SHK, N 33 ad art. 16 LDA.
106 DE WERRA, CR-PI, N 9 ad art. 16 LDA.
107 DE WERRA, CR-PI, N 7 ad art. 16 LDA.

utilisateurs dont il connaît l'activité suffit pour qu'un transfert intervienne valablement[108].

La complexité de la question augmente du fait que les droits d'auteur, même sur des œuvres futures, peuvent être cédés à une société de gestion collective qui les acquiert alors à titre fiduciaire, mais de manière exclusive[109], et peut les faire valoir à l'encontre des tiers de bonne foi[110] auxquels l'auteur aurait subséquemment transféré ces mêmes droits. Force est donc de constater que si, en dehors de la règle spécifique de l'art. 17 LDA pour les « logiciels de service », la liberté contractuelle prévaut[111] en matière de transfert de droits d'auteur portant sur d'autres types d'œuvre, la sécurité du droit n'y gagne pas.

a) L'obligation de rendre compte et de restituer et acte de disposition préalable

L'art. 332 CO, comme aussi l'art. 17 LDA, sont le fruit d'un arbitrage entre le principe du créateur[112] et l'intérêt de l'employeur à pouvoir disposer des résultats de l'activité dont il a supporté le risque économique et qui a été déployée à son profit par ses employés[113].

Les dispositions sur l'obligation de rendre compte et de restituer du travailleur (art. 321*b* CO), qui sont une concrétisation de son devoir général de diligence et de fidélité (art. 321*a* CO)[114] et qui impliquent (art. 321*b* al. 2 CO) que le travailleur remette

---

108 TF 4A_104/2008 du 8 mai 2008, in : sic ! 10/2008, p. 713-717, « SBB-Uhren IV » ; RUEDIN/DUBOIS/TISSOT, n° 21.

109 DE WERRA, CR-PI, N 10 ad art. 16 LDA. Un tel contrat entre société de gestion collective et auteur pourrait avoir été valablement conclu avant même l'engagement de l'auteur comme salarié au sein d'une entreprise et empêcher son employeur d'utiliser les droits d'auteur portant sur les « œuvres de service » sans verser à la société de gestion collective cessionnaire des droits futurs une indemnité tarifaire supplémentaire au salaire servi au travailleur ; voir dans ce sens ALDER, p. 502.

110 DE WERRA, SHK, N 10 ad art. 16 LDA ; voir ATF 117 II 463, JdT 1992 I 393 (rés.), et BARRELET/EGLOFF, N 25 ad art. 16 LDA, sur le fait qu'il n'y a pas en matière de transfert des droits d'auteur d'apparence juridique à laquelle la protection de la bonne foi puisse se rattacher.

111 Voir sur les limites à la liberté contractuelles découlant des art. 19 al. 2 CO et 27 CC et sur leurs effets sur un éventuel transfert des droits moraux (exclus par la jurisprudence du TF), « Guide orange », in : sic ! 7/8/2010, p. 526-530, consid. 3.3, non publié aux ATF ; DE WERRA, CR-PI, N 13 et N 16 ad art. 16 LDA ; DE WERRA, SHK, N 15a ad art. 16 LDA et *infra* III.B.3.c.

112 Voir *supra* III.B.1.

113 Voir dans ce sens, TISSOT, Commentaire, N 1 ad art. 332 CO et TISSOT, CR-PI, N 31 ad art. 3 LBI.

114 ALDER, p. 481 ; voir aussi DUNAND, N 2 ad art. 321*a* CO et N 2 ad art. 321*b* CO.

immédiatement à l'employeur tout ce qu'il a produit par son activité contractuelle[115], ne justifient pas sans autre une dérogation au principe du créateur[116].

Il convient dès lors que l'accord intervenu entre les parties au moment de la conclusion du contrat de travail règle spécifiquement cette question ou reflète au moins la volonté des parties de permettre à l'employeur, qui paie son travailleur pour qu'il déploie une activité créatrice, d'utiliser le résultat de son travail, même s'il est protégé par des droits d'auteur. Si l'analyse du rapport contractuel des parties démontre que celles-ci ont entendu, par la conclusion du contrat de travail, permettre à l'employeur de bénéficier des droits d'utilisation sur les résultats de l'activité contractuelle déployée par le travailleur, on est en présence d'un acte de disposition préalable, portant sur des œuvres futures[117], constituant une dérogation conventionnelle au principe du créateur[118]. L'existence d'un acte de disposition préalable doit ainsi être retenue, en l'absence de disposition contractuelle expresse, quand l'application du principe de la confiance permet d'admettre qu'en contractant les parties envisageaient que les droits d'auteur

115 Voir dans ce sens et sur les relations entre l'art. 321*b* al. 2 CO et les règles sur la spécification (art. 726 al. 1 CC), DUNAND, N 13 et 14 ad art. 321*b* CO.

116 Voir dans ce sens WYLER, p. 383 et réf. citées et ALDER, p. 482, qui indique que « Le devoir de restitution ne constitue pas une base légale suffisante pour permettre à l'employeur d'obtenir les droits d'utilisation sur les résultats du travail protégés par le droit d'auteur nécessaires à son entreprise ». Si toutefois il résulte du contrat de travail ou de son interprétation que les parties ont convenu d'un transfert des droits d'auteur, « l'obligation de restituer à la fin des rapports de travail porte aussi sur les esquisses, projets, réalisations partielles qui sont, selon leur degré d'individualité, protégés par le droit d'auteur », voir dans ce sens ALDER, p. 507.

117 Voir sur l'admissibilité d'accord de cession des droits d'auteur sur des œuvres futures, DE WERRA, CR-PI, N 15 ad art. 16 LDA et BARRELET/EGLOFF, N 9 ad art. 16 LDA ; voir aussi concernant un transfert des droits d'auteur en relation avec des modes d'utilisations futures, BARRELET/EGLOFF, N 9 ad art. 16 LDA ; DE WERRA, CR-PI, N 30-32 ad art. 16 LDA et DE WERRA, SHK, N 28-29 ad art. 16 LDA.

118 Qui ne saurait être assimilé à une « cession automatique des droits patrimoniaux » en dépit du silence qualifié du législateur, voir SEILER, p. 101 et 102 ; ANDERMATT, p. 289, qui propose, en lien avec les inventions et les designs de travailleurs, d'opter lorsque la volonté des parties sur le transfert des droits n'est pas claire pour l'existence d'un acte de disposition préalable seul conforme à « l'économie » du contrat de travail, ne paraît par contre pas pouvoir être suivi lorsque des droits d'auteur sont concernés et que les créations considérées ne sont pas des œuvres de service. Voir en particulier BARRELET/EGLOFF, N 22a ad art. 16 LDA et SEILER, p. 109, qui précise, p. 112, que « si le contrat comporte une lacune et qu'elle porte sur un point essentiel, tel que le principe même de la cession, le juge ne pourra pas la combler, ni admettre un transfert des droits d'auteur en l'absence d'un accord des parties sur les éléments essentiels du transfert des droits » ; voir aussi *infra* note 122.

d'utilisation sur les œuvres futures créées par l'employé dans le cadre de son activité contractuelle reviendraient à l'employeur[119].

Dans une décision récente[120], le TF a précisé qu'un transfert de droits d'auteur peut parfaitement être conclu tacitement, voire par actes concluants, et que pour savoir s'il est intervenu le juge doit en premier lieu recourir « à l'interprétation subjective qui le contraint à rechercher la commune et réelle intention des parties, sans s'arrêter aux expressions ou dénominations inexactes dont elles ont pu se servir soit par erreur, soit pour déguiser la nature véritable de la convention [art. 18 al. 1 CO]. […] Si la volonté réelle des parties n'a pas pu être déterminée ou si les volontés intimes de celles-ci divergent », il convient de passer à une interprétation objective des déclarations et des comportements selon la théorie de la confiance, ce qui oblige le juge « à rechercher comment une déclaration ou une attitude pourrait être comprise de bonne foi en fonction de l'ensemble des circonstances. Le principe de la confiance permet d'imputer à une partie le sens objectif de sa déclaration ou de son comportement, même s'il ne correspond pas à sa volonté intime […]. Lorsque l'interprétation objective aboutit à une ambiguïté, il est possible de faire application de la théorie de la finalité ». Ce n'est donc que conjointement avec les autres méthodes d'interprétation et en quelque sorte en « dernier recours » que la théorie de la finalité trouve application lorsqu'il s'agit de déterminer si les parties avaient ou non la volonté de déroger conventionnellement au principe du créateur.

Parmi les critères dont la réunion débouche sur l'admission de l'existence d'une volonté de transférer les droits d'auteur à l'employeur, la doctrine mentionne en particulier le fait que l'employé a été engagé et payé pour la création des œuvres, qu'il a pu bénéficier pour leur réalisation d'une intégration dans l'entreprise de l'employeur (dont il a le cas échéant pu utiliser l'infrastructure), et que leur utilisation entre dans le domaine d'activité de l'employeur[121]. La satisfaction de ces conditions revient *de facto* à définir

---

119 Voir dans ce sens, ANDERMATT, p. 290. BARRELET/EGLOFF se montrent très restrictifs quant à la possibilité de recourir à la théorie de la finalité pour déterminer si un contrat de travail qui ne règle pas expressément la question du transfert des droits d'auteur peut néanmoins déboucher sur une cession des droits d'auteurs. Ils indiquent ainsi, N 22a ad art. 16 LDA, « […] si le contrat de travail ne règle rien, il n'y a pas de transfert des droits d'auteur. A titre exceptionnel, un transfert peut être déduit du but contractuel poursuivi, si celui-ci fait référence à une utilisation déterminée de l'œuvre à créer ».

120 TF 4A_643/2012 du 23 avril 2013, consid. 3.1, in : sic ! 10/2013, p. 605 ss, « Reportages SSR ».

121 Voir dans ce sens ALDER, p. 483 et 490-491 ; voir aussi SEILER, p. 103 ss, qui relève, p. 106, que « lorsque le créateur est salarié d'une entreprise dont l'activité principale ou régulière est la production et l'exploitation d'œuvres, le principe du transfert des droits d'auteur apparaîtra généralement comme évident ».

une forme d'« œuvres de service » qui seule peut faire l'objet d'un acte de disposition préalable[122].

Pour les œuvres « occasionnelles ou réservées et libres », la cession conventionnelle des droits d'auteur doit être explicite et ne peut être déduite du but poursuivi par les parties en contractant[123]. A défaut de dispositions contractuelles expresses, il ne sera pas possible de retenir, selon le principe de la confiance, un transfert des droits d'auteur les concernant. Il paraît en effet exclu que les parties, qui n'avaient pas prévu que le travailleur aurait à se montrer créatif et qui n'avaient aucun intérêt à envisager que son activité déboucherait sur un résultat protégé par le droit d'auteur mais ne présentant aucune utilité pour l'employeur, auraient voulu, par leur accord, transférer à l'employeur les droits d'auteur portant sur ces créations dont elles n'avaient anticipé ni la réalisation, ni l'utilité. Il convient de se rappeler que la recherche, selon l'approche objective, de la volonté présumée des parties ne peut intervenir en matière de transfert de droits d'auteur que « si un transfert des droits a été voulu de part et d'autre, sans qu'on soit en présence d'une volonté concordante des parties »[124]. Or, pour qu'un transfert ait été voulu par les parties, il faut qu'elles aient eu une raison de l'envisager et un intérêt à le décider.

Lorsque le travailleur demeure investi des droits d'auteur sur les résultats de son travail, tout au plus peut-il être tenu dans la mesure où il décide de les valoriser et où l'utilisation de l'œuvre entre dans le domaine d'activité de l'entreprise, d'en proposer l'utilisation à son employeur « avant son exploitation par un tiers et de la lui laisser à offre égale »[125], soit moyennant le paiement d'un prix ne correspondant pas au seul salaire déjà versé[126]. Selon la doctrine apparemment majoritaire en droit d'auteur, si l'interprétation du contrat permet d'établir l'existence d'un acte de disposition préalable, l'employeur ne sera titulaire qu'à titre dérivé des droits d'auteur sur les résultats du travail de son employé,

---

122 DE WERRA, CR-PI, N 45 ad art. 16 LDA, admet, pour les œuvres de service, « la cession des droits d'utilisation dans la mesure nécessaire au but du contrat de travail ». En relation avec ces types de créations particulières, il relève, N 45 ad art. 16 LDA, que « dans le cas où la volonté subjective des parties au contrat ne peut pas être déterminée, il convient ainsi de partir du principe que l'employé a cédé à l'employeur tous les droits sur l'œuvre dont l'employeur a besoin pour atteindre son but ».

123 Voir dans ce sens ANDERMATT, p. 291 et ALDER, p. 491 et 492.

124 BARRELET/EGLOFF, N 21 ad art. 16 LDA, qui précisent que l'application de la théorie de la finalité ne doit pas avoir pour effet de pallier à l'absence de volonté des parties de transférer les droits d'auteur.

125 Voir dans ce sens ANDERMATT, p. 291 et ALDER, p. 486 et 492.

126 Voir dans ce sens et pour une analogie avec les inventions libres, TISSOT, Commentaire, N 19 ad art. 332 CO et réf. citées ; voir aussi pour le principe du versement d'une indemnité additionnelle au salaire, par analogie à ce que prévoit l'art. 332 al. 4 CO, ANDERMATT, p. 291.

dont il sera toutefois investi dès l'instant même de l'achèvement de l'œuvre, sans qu'aucun acte de transfert de la part de l'employé ne soit nécessaire[127].

Une fois l'existence d'un acte de disposition préalable établie, la théorie de la finalité permet encore de préciser l'étendue de la cession des droits d'auteur concernés[128].

b) La théorie de la finalité et l'étendue des droits cédés

Ainsi que cela vient d'être rappelé, la théorie de la finalité a une portée plus large que la seule détermination de l'étendue des droits cédés selon l'art. 16 al. 2 LDA[129] et constitue une règle d'interprétation qui a valeur prépondérante « aussi bien pour la cession des droits d'auteur que la reconnaissance de certains droits d'utilisation »[130].

Il est toutefois nécessaire d'être en présence d'un contrat à interpréter pour que l'application de la théorie de la finalité entre en ligne de compte. Tel n'est pas le cas si « la réelle volonté des parties au contrat ne laisse pas de place à l'interprétation du contrat »[131]. Si le contrat a un contenu clair, « c'est lui qui sera déterminant, indépendamment du but concret du contrat. Si ni un transfert de droits d'auteur, ni la cession de droits d'utilisation n'est prévu par le contrat, il n'y aura rien à interpréter »[132]. « Si le contrat est lacunaire sur un élément non essentiel, il incombe au magistrat de préciser cet élément. Le juge pourra décider, par exemple, de l'étendue des droits d'auteur cédés en fonction de la volonté hypothétique des parties »[133]. Il est ainsi admis « qu'en cas de doute concernant l'étendue de la cession, l'auteur ne cède pas plus de droits d'auteur que le but du contrat ne l'exige »[134]. En outre, et sauf convention

---

127 Voir dans ce sens ANDERMATT, p. 290-291 ; SEILER, p. 102 et réf. citées et DE WERRA, CR-PI, N 46 ad art. 16 LDA. Dans le cas pourtant similaire où un acte de disposition préalable permet de déroger au principe de l'inventeur en droit des brevets, il est par contre admis que le droit au brevet naît au moment de l'achèvement même de l'invention en la personne du tiers acquéreur auquel il appartient à titre originaire ; voir dans ce sens TISSOT, CR-PI, N 20 ad art. 3 LBI et réf. citées.

128 TF 4A_643/2012 du 23 avril 2013, consid. 3.1, in : sic ! 10/2013, p. 605 ss, « Reportages SSR », voir en particulier ANDERMATT, p. 291.

129 Voir DE WERRA, CR-PI, N 42 et 43 ad art. 16 LDA.

130 BARRELET/EGLOFF, N 20 ad art. 16 LDA.

131 DE WERRA, CR-PI, N 41 ad art. 16 LDA.

132 BARRELET/EGLOFF, N 21 ad art. 16 LDA.

133 SEILER, p. 112.

134 DE WERRA, CR-PI, N 41 ad art. 16 LDA, voir aussi TF 4A_643/2012 du 23 avril 2013, consid. 3.1, in : sic ! 10/2013, p. 605 ss, « Reportages SSR », qui relève que « si l'interprétation selon la « théorie de la confiance laisse subsister un doute sur la volonté normative des parties, il faut partir de l'idée que l'auteur n'a pas cédé plus de droits liés aux droits d'auteur que ne le requiert le but poursuivi par le contrat, selon la théorie de la finalité » ; et que « conformément à celle-ci et à la teneur de l'art. 16

contraire, le transfert d'un des droits partiels n'implique pas celui des autres droits partiels (art. 16 al. 2 LDA)[135].

Ainsi, l'employeur qui voudrait s'assurer la possibilité d'exploiter licitement le site web ou le compte créé par ses employés sera bien avisé d'intégrer dans le contrat de travail de ces derniers une clause spécifiant au moins que le droit de reproduction (art. 10 al. 2 let. a LDA), celui de communication publique (art. 10 al. 2 let. c LDA), ainsi que celui de créer une œuvre dérivée (art. 11 al. 1 let. a LDA) lui sont transférés. Il convient, dans l'énumération faite des droits concernés par la cession envisagée, de conserver à l'esprit que l'application de l'art. 16 al. 2 LDA pourra aussi avoir pour effet de permettre de déterminer « quels autres droits partiels (distincts de ceux qui ont été identifiés et cédés) n'ont pas été cédés »[136]. Dès qu'il découle de la volonté réelle et concordante des parties que la cession convenue est totale, l'art. 16 al. 2 LDA n'a cependant plus vocation à s'appliquer[137], d'où l'utilité de prévoir une clause large de cession plutôt que de chercher à énumérer ceux des droits partiels transférés.

Il est enfin utile de se souvenir que « le transfert de la propriété d'une œuvre n'implique pas celui des droits d'auteur [art. 16 al. 3 LDA], mais que la jurisprudence a admis que la remise des exemplaires d'une œuvre commandée […] peut comporter la cession tacite des droits d'auteur sur cette œuvre »[138]. La remise par des employés à leur employeur du « *lay out* » d'un site Internet, ainsi que des textes, images et musiques qui l'animent, pour que le site puisse être activé ; puis le fait de tolérer, au moins pendant un certain temps, son exploitation par leur employeur devraient ainsi, au vu de la jurisprudence[139], déboucher sur une cession tacite des droits d'auteur de reproduction, de communication publique et le cas échéant d'utilisation pour en faire une œuvre dérivée (pour le texte, la musique et les images qui seront « fondus » dans l'œuvre multimédia globale que constitue le site lui-même).

---

al. 2 LDA, en cas de doute, l'interprétation des contrats de droits d'auteur doit pencher en faveur de la personne protégée (« *in dubio pro auctore* ») ».

135 DE WERRA, CR-PI, N 48 ad art. 16 LDA.

136 DE WERRA, CR-PI, N 50 ad art. 16 LDA.

137 Le recours à la théorie de la finalité n'intervenant qu'en complément aux autres méthodes d'interprétation lorsque la volonté réelle et concordante des parties ne peut pas être déterminée, voir *supra* III.B.3.a) et DE WERRA, CR-PI, N 50 ad art. 16 LDA.

138 Voir DE WERRA, CR-PI, N 54 ad art. 16 LDA et jurisprudence citée, ainsi que TF 4A_643/2012 du 23 avril 2013, consid. 3.2, in : sic ! 10/2013, p. 605 ss, « Reportages SSR », concernant la remise par leur auteur de reportages protégés par le droit d'auteur à une institution dont le but est d'émettre des émissions de radio.

139 Voir RUEDIN/DUBOIS/TISSOT, n° 20-23 et 25.

L'art. 16 al. 2 LDA ne porte que sur l'étendue matérielle d'une cession, mais la théorie de la finalité permet aussi de trancher la question de sa durée[140]. La doctrine considère qu'à moins que les parties en aient convenu autrement, la fin des rapports de travail est dépourvue d'incidence sur la cession des droits d'auteur et les limitations contractuelles au droit de sa personnalité que l'auteur doit admettre pour permettre à l'employeur d'exercer les droits d'utilisation dont il est investi[141]. La cession continue donc de déployer ses effets même après la fin du contrat de travail « car le versement du salaire est une indemnisation de l'activité déployée [par le travailleur] qui a entre autres conduit à des résultats du travail [protégés ou pas par des droits de propriété intellectuelle] et ne constitue pas la contre-prestation d'un droit à bénéficier d'une licence pendant la durée des relations de travail »[142]. Cela est aussi conforme au fait que l'intérêt de l'employeur à pouvoir exploiter le site ou le compte concerné, que prend en compte la théorie de la finalité, demeure après l'échéance des rapports de travail. Dans le même ordre d'idée, « l'employé qui quitte l'entreprise ne devrait pas pouvoir s'opposer à ce qu'un de ses collègues termine l'œuvre qu'il était en train de réaliser »[143].

Enfin, le montant de la rémunération touchée par le travailleur joue un rôle dans « l'établissement de la volonté présumée ou hypothétique des parties (…). Plus la rémunération est élevée, plus le salarié peinera à affirmer de bonne foi n'avoir autorisé aucun usage étendu de son œuvre par l'employeur »[144]. L'usage dans la branche peut aussi, en tant que concrétisation du but poursuivi par les parties en contractant dans ce domaine précis, justifier un transfert du droit d'auteur[145].

Comme le système de l'art. 332 CO n'est pas transposable à la cession des droits d'auteur dans le cadre d'un contrat de travail, et comme aussi, si elle est implicite, la cession ne peut porter que sur des « œuvres de service »[146], le salarié ne bénéficie alors d'aucune prétention additionnelle à son salaire[147]. En l'absence toutefois d'un acte de disposition préalable, l'utilisation de l'œuvre par l'employeur qui n'y est pas

140 Voir DE WERRA, CR-PI, N 49 ad art. 16 LDA.
141 Voir dans ce sens, ALDER, p. 507.
142 Traduction libre de ALDER, p. 507.
143 Traduction libre de ALDER, p. 507.
144 SEILER, p. 110-111.
145 SEILER, p. 111.
146 A noter que le travailleur qui réalise une invention de service n'a aussi, sauf disposition contractuelle contraire, pas droit à une indemnité particulière additionnelle à son salaire, voir TISSOT, Commentaire, N 12 ad art. 332 CO.
147 Voir dans ce sens pour l'absence de rémunération supplémentaire en lien avec le bénéfice d'un droit d'utilisation sur les créations de service non spécifiquement réglées par des dispositions spéciales de propriété intellectuelle, soit en particulier les droits d'auteur portant sur des œuvres autres que les logiciels, WYLER, p. 384 et SEILER, p. 114.

expressément autorisé par le contrat de travail intervient en violation des droits d'auteur de l'auteur salarié qui « aura droit à une compensation non pas sous forme de rémunération pour l'utilisation de ses droits, mais de dommages et intérêts »[148].

c) L'absence de cession des droits moraux

Seuls les droits patrimoniaux peuvent, le cas échéant, faire l'objet d'une cession en application de la théorie de la finalité. Les droits moraux eux sont incessibles[149]. Le TF a en effet précisé que le droit moral ne peut être cédé puisqu'il est indissociablement lié à la personne physique qui a qualité d'auteur et que l'intérêt d'une telle personne à faire constater qu'elle est l'auteur d'une œuvre déterminée existe toujours et ne saurait disparaître par l'écoulement du temps[150]. S'il ne peut céder ses droits moraux, l'auteur peut par contre « autoriser l'exercice des prérogatives qui en découlent dans des cas particuliers »[151]. Ainsi, « la question de la cessibilité du droit moral ne peut être traitée de façon abstraite […], elle doit être étudiée spécialement selon le droit moral concerné »[152] et en fonction des circonstances particulières à chaque cas comme par exemple de la nature de l'œuvre (fonctionnelle ou pas) et des conditions qui ont présidé à sa création (œuvre créée sur commande ou de façon indépendante par exemple)[153]. « En principe, l'auteur employé conserve le droit de revendiquer la paternité de l'œuvre »[154]. Seule une renonciation à faire valoir ce droit entre donc en ligne de compte[155]. Elle est limitée à ceux des droits moraux dont l'exercice doit être restreint pour permettre l'utilisation de l'œuvre dans le cadre convenu[156].

---

148 SEILER, p. 114.

149 BARRELET/EGLOFF, N 6 ad art. 16 LDA et DE WERRA, CR-PI, N 16 ad art. 16 LDA.

150 TF 4A_638/2009 du 1er avril 2010, consid. 3.3 *in fine* et RUEDIN/DUBOIS/TISSOT, n° 6.

151 BARRELET/EGLOFF, N 6 ad art. 16 LDA.

152 DE WERRA, CR-PI, N 21 ad art. 16 LDA.

153 DE WERRA, CR-PI, N 19 ad art. 16 LDA, voir aussi sur la controverse doctrinale qui a précédé l'arrêt du TF 4A_638/2009 du 1er avril 2010, et sur la nécessité de trancher au cas par cas de la validité d'un transfert ou d'une renonciation à faire valoir ses droits, DE WERRA, SHK, N 15a-20 ad art. 16 LDA.

154 CHERPILLOD, CEDIDAC, p. 109, qui relève qu'« on se trouve souvent en présence de cas dans lesquels il est présumé y renoncer ».

155 Voir dans ce sens, DE WERRA, CR-PI, N 24 ad art. 16 LDA. A relever que dans le cas des inventions de service aussi, « même s'il est investi à titre originaire du droit au brevet, l'employeur est tenu de respecter le droit à la mention de l'inventeur de l'art. 5 LBI puisque l'exception au principe de l'inventeur introduite par les art. 3 al. 1 LBI et 332 al. 1 CO, ne concerne que les aspects patrimoniaux des droits revenant à l'inventeur » ; TISSOT, Commentaire, N 11 ad art. 332 CO et réf. citées.

156 Voir dans ce sens ALDER, p. 505 et aussi p. 494-495 sur les limitations à l'exercice des droits moraux découlant du contexte particulier des œuvres réalisées dans le cadre d'un contrat de travail dont l'obligation de diligence et de fidélité entrave plus le travailleur dans l'exercice des droits moraux que le principe général de la bonne foi qui vaut dans les relations contractuelles d'un autre type.

C. La réalisation de la plateforme par des tiers externes

Le plus souvent, le développement de toute la partie logicielle et multimédia d'un site ou d'un compte web sera confié par l'entreprise à des tiers externes plutôt qu'à ses employés dont les compétences ne permettent, sauf cas particulier, pas ce type de réalisation. Que le contrat de développement de la plateforme Internet soit un contrat de mandat ou un contrat d'entreprise, il conviendra à nouveau, à défaut de cession expresse, claire et globale des droits d'auteur, de chercher à déterminer si par la conclusion du contrat les parties ont voulu déroger au principe du créateur. La liberté contractuelle le leur permet et il s'agira de procéder de la même manière que dans le cadre d'un contrat de travail pour déterminer si la conclusion du contrat constitue un acte de disposition préalable ou pas[157]. Ce n'est ainsi qu'en l'absence de clause de cession claire et expresse dans le contrat à l'origine de la réalisation de la plateforme et pour autant que l'application des méthodes d'interprétation subjective, puis éventuellement objective avec l'application du principe de la confiance et encore le cas échéant le recours à la théorie de la finalité, ne permette pas d'admettre que le but poursuivi par les parties en contractant était de déroger au principe du créateur que celui-ci s'appliquera, et que les droits d'auteur demeureront en la personne du prestataire de service[158].

IV. Conclusion

Un site Internet ou un compte sur un réseau social n'est pas assimilable à un logiciel au sens du droit d'auteur. Chaque élément du compte ou du site fait l'objet d'une protection séparée, s'il constitue une œuvre au sens de l'art. 2 LDA, si bien que le transfert des droits à l'employeur doit être examiné séparément pour chacun de ces éléments. Pour les logiciels de service intégrés dans le site ou le compte, l'art. 17 LDA a pour conséquence que l'employeur est seul autorisé à exercer les droits. En revanche, pour les autres apports protégés, la cession nécessite une base contractuelle, l'art. 332 CO n'étant pas applicable. Pour déterminer si une telle base contractuelle existe, il faudra d'abord recourir à l'interprétation subjective, c'est-à-dire rechercher la commune et réelle intention des parties. Si cette volonté réelle ne peut pas être déterminée, ou si les volontés des parties divergent, le juge devra recourir à la théorie de la confiance, ce qui l'obligera à rechercher comment une déclaration ou une attitude pouvait être comprise de bonne foi en fonction de l'ensemble des circonstances (interprétation objective). Si une ambiguïté

157 Voir III.B.3.a).

158 Voir pour une solution analogue en lien avec le principe de l'inventeur en droit des brevets, TISSOT, CR-PI, N 21-23 ad art. 3 LBI.

subsiste, il sera alors possible de recourir à la théorie de la finalité, c'est-à-dire rechercher quels sont ceux des droits partiels qui doivent passer à l'employeur pour permettre aux parties d'atteindre le but poursuivi en contractant, et présumer que l'auteur n'a pas cédé plus de droits que ne le requiert ce but.

Dès lors, on ne saurait trop recommander aux employeurs de régler expressément et de manière claire, dans les contrats de travail qu'ils proposent, la cession des droits sur les apports créatifs de leurs employés concernant la réalisation d'un site Internet ou l'ouverture d'un compte sur un réseau social. De plus, l'employeur devra être particulièrement attentif à ce que ses travailleurs acquièrent de manière régulière les droits sur les œuvres préexistantes utilisées pour un tel site ou un tel compte. Faute d'acquisition régulière, il y aurait en effet un acte illicite au sens des art. 41 ss CO, dont l'employeur pourrait répondre en vertu de l'art. 55 CO.

V. Bibliographie

ALDER DANIEL, Urheberrecht und Arbeitsvertrag, in : STREULI-YOUSSEF (édit.), Urhebervertragsrecht, Berne 2006.

ANDERMATT ADRIAN, Die arbeitsrechtliche Zuordnung von immaterialgüterrechtlich geschützten Arbeitsergebnissen, RSJ 104 (2008), p. 284 ss.

BARRELET/EGLOFF, Le nouveau droit d'auteur, Commentaire de la loi fédérale sur le droit d'auteur et les droits voisins, 3e éd., Berne 2008.

BUEHLER LUKAS, Schweizerisches und internationales Urheberrecht im Internet, Fribourg 1999.

CHERPILLOD IVAN, Titularité et transfert des droits, in : MARCHETTO (édit), La nouvelle loi fédérale sur le droit d'auteur, CEDIDAC, Lausanne 1994 (cité : Cherpillod, CEDIDAC).

CHERPILLOD IVAN, in : MÜLLER/OERTLI (édit.), Urheberrechtsgesetz (URG), Stämpflis Handkommentar SHK, 2e éd., Berne 2012 (cité : Cherpillod, SHK).

CHERPILLOD IVAN, Commentaire romand de la propriété intellectuelle, à paraître en 2013 (cité : Cherpillod, CR-PI).

DE WERRA JACQUES, in : MÜLLER/OERTLI (édit.), Urheberrechtsgesetz (URG), Stämpflis Handkommentar SHK, 2e éd., Berne 2012 (cité : de Werra, SHK).

DE WERRA JACQUES, Commentaire romand de la propriété intellectuelle, à paraître en 2013, (cité : de Werra, CR-PI).

DUNAND JEAN-PHILIPPE, in : DUNAND/MAHON (édit.), Commentaire du contrat de travail, Berne 2013.

GILLIÉRON PHILIPPE, Propriété intellectuelle et Internet, CEDIDAC, Lausanne 2003.

HILTY RETO M., Urheberrecht, Berne 2011.

RENOLD MARC-ANDRÉ, Internet et le droit d'auteur, SJ 2002, p. 83 ss.

ROBERT VINCENT, Enjeux juridiques des médias sociaux, Journée CEDIDAC du 14 mai 2013 sur les « développements récents dans l'environnement numérique », Lausanne 2013.

RUEDIN/DUBOIS/TISSOT, Propriété Intellectuelle, jurisprudence fédérale et cantonale, 2007-2011, Neuchâtel 2013.

SEILER ZOE, Œuvres et contrat de travail, interprétation en cas de litige, SJ 2012, II.

TISSOT NATHALIE, Commentaire romand de la propriété intellectuelle, à paraître en 2013 (cité : Tissot, CR-PI).

TISSOT NATHALIE, in : DUNAND/MAHON (édit.), Commentaire du contrat de travail, Berne 2013 (cité : Tissot, Commentaire).

WYLER RÉMY, Droit du travail, 2e éd., Berne 2008.

OLIVIER SUBILIA

Du papier à l'électronique : quels changements ?

Cher Maître, je vous envoie ce SMS pour que vous preniez connaissance de mon récent courriel dans lequel je vous confirme l'envoi d'une correspondance préadressée par télécopie.

M. Bolomey, client inquiet

Sommaire

		Page
I.	Correspondance électronique (courriel)	256
A.	Courriel (ordinaire) signé électroniquement	257
1.	Notions techniques	257
2.	En pratique	258
a)	Difficultés techniques	259
b)	Absence d'intérêt pratique	259
B.	Courriel recommandé	260
1.	Système d'expédition et de réception	261
2.	Conséquences juridiques de la (non-) réception	262
a)	Réception du message par son destinataire	263
b)	Non-réception du message par son destinataire	264
c)	Synthèse	265
II.	SMS	266
III.	Informations officielles	267
IV.	Stockage et l'archivage électroniques	268
A.	Avantages de l'électronique	268
B.	Inconvénients de l'électronique	269
1.	Conservation et authenticité des données	269
2.	Problème de protection des données	270
V.	Communications avec les autorités	272
A.	Procédure cantonale	272
B.	Recours devant le Tribunal fédéral	272
1.	Problèmes généraux de forme	273
2.	Nécessité d'une inscription	274

3. Utilisation obligatoire d'une transmission « recommandée » et transfert des risques 274
4. Emploi du recours électronique dans la pratique 276

VI. Conclusion 277

VII. Bibliographie sommaire 278

Depuis quelques années, la communication électronique est devenue sinon la règle, du moins une généralité. Dans les entreprises, le courriel tend à remplacer le papier, les documents sont transmis sous forme de fichiers pour traitement de texte ou pour visionneuse à l'écran plutôt que de liasses de feuilles. La signature numérique est désormais régie par le droit fédéral. On peut commander son certificat à une poste de quartier ou sur le site de la Poste Suisse[1]. On peut archiver ses dossiers par le biais d'un scanner et stocker ses données de manière à les rendre accessibles quel que soit son lieu de travail.

Si le numérique a progressé, qu'en est-il de la réglementation qui lui est applicable ? L'utilisateur peut-il sans autre considérer son courriel comme une lettre manuscrite ou dactylographiée ? Le stockage des données sous forme de bits répond-il aux mêmes règles que l'archivage de documents papier dans une cave ?

Nous proposons ci-après un bref survol des dispositions spécifiques applicables aux documents numériques.

I. Correspondance électronique (courriel)

Jusqu'à une époque récente, on qualifiait de correspondance l'échange de documents écrits, adressés par un expéditeur à un destinataire. Aujourd'hui, tout ordinateur (voire téléphone) permet d'envoyer des messages par de multiples moyens sans édition d'un document physique. Citons notamment le courriel, le SMS et les divers médias sociaux (Facebook, Twitter, Linkedin par exemple).

Régulièrement, ces canaux sont utilisés pour des manifestations de volonté auxquelles les parties entendent donner un caractère juridique, qu'il s'agisse de la conclusion d'un contrat ou de l'exercice d'un droit formateur comme une résiliation. Cependant, l'usage courant n'est pas encore l'expression des conséquences juridiques qui y sont attachées.

1 http://www.poste.ch/suisseid (consulté le 16 novembre 2013).

Lorsqu'un acte juridique n'est attaché à aucune forme particulière, chacune de ces manifestations de volonté – sous réserve de sa preuve – sera propre à faire naître une conséquence juridique. Ainsi il est possible de conclure un contrat de travail par SMS ou de le résilier par courriel, de la même manière que ces actes peuvent être conclus oralement.

Autre est la question de savoir si une correspondance électronique peut se voir reconnaître les mêmes effets qu'un document écrit ; c'est ce que nous examinons ci-après.

A. Courriel (ordinaire) signé électroniquement

De façon générale, la forme écrite se définit par la signature de la personne qui s'engage sur le document. Selon l'art. 14 al. 2bis CO, la signature électronique qualifiée, basée sur un certificat qualifié émanant d'un fournisseur de services de certification reconnu au sens de la Loi sur la signature électronique[2] est assimilée à la signature manuscrite. *A contrario*, pour être qualifié de titre, un courriel doit porter une signature électronique qualifiée.

1. Notions techniques

Techniquement, une signature électronique correspond à un procédé de chiffrement. La personne désireuse de prouver son identité et l'intégrité des messages qu'elle envoie se procure deux « clés » électroniques : chacune des clés est telle qu'elle permet de décoder ce que l'autre a codé, mais ne permet pas de décoder ce qu'elle a elle-même codé. L'une des clés est dite publique et connue virtuellement du monde entier. L'autre, privée, est conservée secrète. Lorsqu'un utilisateur veut signer un message, il commence par créer pour ce message ce qu'on appelle une somme de contrôle, soit une succession de caractères obtenue par la transformation du message via une fonction publiquement connue, de sorte qu'un texte déterminé donnera toujours la même somme de contrôle[3]. Il crypte ensuite cette somme avec sa clé privée, le résultat constituant sa signature électronique. Le destinataire décrypte cette signature avec la clé publique de l'expéditeur et obtient la somme de contrôle calculée par l'expéditeur. Il calcule enfin lui-même la

2 Loi fédérale du 19 décembre 2003 sur les services de certification dans le domaine de la signature électronique (SCSE, RS 943.03).

3 En théorie, puisque la somme de contrôle est nettement plus courte que le message, il est possible d'obtenir une même somme avec plusieurs textes différents. En pratique, même des algorithmes dits « peu sûrs » (hachage MD5, par exemple) donnent des sommes de contrôle d'une taille de 128 bits, soit quelque 340 milliards de milliards de milliards de milliards de possibilités, alors que l'algorithme SHA-1 utilisé dans la SwissID multiplie encore ces possibilités par 4 milliards environ. La probabilité de trouver un texte différent du premier, malgré tout cohérent et donnant la même somme de contrôle est ainsi négligeable.

somme de contrôle sur le message reçu. Si les deux résultats sont identiques, cela signifie que l'expéditeur est bien le détenteur de la clé privée et que le message n'a pas été altéré[4].

Néanmoins, ce procédé est inutile si l'on ne peut pas garantir que la clé publique qui correspond à la clé privée de départ appartient bien à un expéditeur dont l'identité est attestée[5]. Il faut donc que les clés de l'utilisateur soient elles-mêmes signées par un organisme de confiance certifiant que le propriétaire d'une clé numérique est bien une personne physique ou morale connue. A ce jour, quatre organismes en Suisse sont légalement autorisés[6] à délivrer des identités numériques : Swisscom (Suisse) SA, Quo Vadis Trustlink Schweiz AG, SwissSign AG et l'Office fédéral de l'informatique et de la télécommunication. Ces mêmes autorités doivent être accréditées par un organisme au sens de l'art. 4 SCSE. Un seul organisme dispose en Suisse du droit d'accréditer ; il s'agit de KPMG[7].

Le système repose ainsi sur une chaîne de confiance : il faut pouvoir s'assurer de l'identité de l'expéditeur, certifiée par l'organisme de délivrance, puis de l'identité de cet organisme, attestée par l'organisme d'accréditation ; enfin, il faut que l'identité de l'organisme d'accréditation soit elle-même attestée. Naturellement, toutes ces vérifications se font de manière automatisée par le logiciel servant à expédier ou recevoir les messages.

2. En pratique

En théorie, le système est assez simple. L'acquisition d'une identité numérique se fait de manière relativement aisée. Les logiciels servant à employer cette identité sont aussi faciles à utiliser qu'à installer. L'utilisation de documents cryptés devrait donc être la règle. Tel n'est cependant guère le cas à ce jour. L'utilisation de données signées demeure marginale, pour de multiples raisons.

---

4 Pour une explication plus complète, voir par exemple : http://www.commentcamarche.net/contents/212-signature-electronique (consulté le 16 novembre 2013) ; http://fr.wikipedia.org/wiki/Signature_ électronique (consulté le 16 novembre 2013).

5 Voir XOUDIS, N 21 ad art. 14 CO et les réf.

6 Art. 14 al. 2bis CO ; art. 3 SCSE ; annexe à l'Ordonnance de l'OFCOM sur les services de certification dans le domaine de la signature électronique disponible à l'adresse http://www.seco.admin.ch/sas/00229/05092/index.html (consulté le 16 novembre 2013).

7 Voir également http://www.seco.admin.ch/sas/00229/05092/index.html (consulté le 16 novembre 2013).

a) Difficultés techniques

L'un des problèmes est que la chaîne de confiance susmentionnée ne fonctionne qu'à la condition que le dernier maillon de la chaîne de confiance soit reconnu par le logiciel de l'utilisateur. Or si l'expéditeur, heureux acquéreur d'une SwissID, doit installer le certificat de confiance pour faire usage de son identité numérique, le destinataire ne reconnaît pas forcément le certificat. Conséquence : l'identité numérique forte de l'expéditeur ne génère aucune confiance chez le destinataire. Juridiquement, la signature est valable. Pratiquement, à moins d'avoir lui aussi adhéré au système préalablement à toute réception, le destinataire voit apparaître l'expéditeur comme « douteux » dans son logiciel de réception[8]. L'on peut bien sûr espérer qu'à terme la situation évoluera : plus le nombre d'utilisateurs du système seront nombreux et plus celui des récepteurs potentiellement convaincus de l'authenticité des messages croîtra. Mais pour l'instant, du point de vue du sentiment de la sécurité des transactions, le système manque complètement sa cible.

b) Absence d'intérêt pratique

La situation du courriel est à l'heure actuelle paradoxale. La loi définit les conditions théoriques auxquelles un courriel peut être assimilé à un titre, mais il n'en est guère fait usage en pratique. Cependant, dans le même temps, le Tribunal fédéral a tendance à considérer un courriel non signé électroniquement (et donc non assimilé à un titre au sens de l'art. 14 CO) comme un titre.

Dans un arrêt à dire vrai quelque peu surprenant[9], le Tribunal fédéral a traité la situation d'une personne qui avait falsifié des courriels (non signés électroniquement) pour en obtenir un avantage pécuniaire indu. Le Tribunal fédéral a jugé que ce procédé était constitutif de faux dans les titres parce que, dans le cas d'un courriel, l'identité de l'expéditeur ressort sinon de l'adresse apparente, du moins du contenu du message[10] ; dès lors, il s'agissait bien d'un titre au sens de l'art. 110 CP.

Cette motivation laisse quelque peu songeur. Il est vrai que le nouveau texte de l'art. 110 al. 4 CP assimile à un document écrit « l'enregistrement sur des supports de données et sur des supports-images s'il a la même destination ». Il ne faut toutefois pas perdre de vue que cette modification date de 1994, à une époque où l'écrit électronique n'existait pas. Pour le législateur de l'époque, « les manipulations de données ne peuvent être

8 Ce d'autant plus que, pour une partie de la doctrine à tout le moins, l'authenticité d'une signature électronique qualifiée ne serait pas présumée. Voir XOUDIS, N 24 ad art. 14 CO.

9 ATF 138 IV 209, JdT 2013 IV 179.

10 ATF 138 IV 209, consid. 5.4, JdT 2013 IV 179.

constitutives de faux dans les titres que dans la mesure où, si elles étaient opérées au moyen de l'écrit traditionnel ou sur celui-ci, elles tomberaient sous le coup des dispositions pénales en matière de titres »[11]. En d'autres termes, il s'agissait d'éviter que la personne qui se servait d'un document électronique ayant la même fonction qu'un document écrit ne soit impunissable en raison du seul support choisi. Néanmoins, si le raisonnement du Tribunal fédéral était compréhensible en 1995, date d'entrée en vigueur des nouvelles normes pénales, il ne l'est plus depuis le 1er janvier 2005[12], date à laquelle le législateur fédéral a voulu clairement distinguer les documents électroniques remplissant la même fonction qu'un écrit de ceux qui n'ont pas ce rôle. En estimant qu'un courriel non signé électroniquement poursuit le même but qu'un document écrit, le Tribunal fédéral réduit à néant l'intérêt du document électroniquement signé par rapport au courriel ordinaire[13].

La situation est encore davantage paradoxale s'agissant du courriel recommandé, comme on l'explique ci-après.

B. Courriel recommandé

De même qu'il existe un courrier recommandé, il est possible d'adresser un courriel recommandé. C'est du reste, le système obligatoirement prévu pour la communication électronique avec les tribunaux[14]. Deux plate-formes sont, à ce jour, admises pour la communication électronique avec les tribunaux[15] : le système mis en place par la Poste Suisse baptisé INCAMail[16] et celui de la société PrivaSphere AG[17].

---

11 FF 1991 II 933, p. 960.

12 Entrée en vigueur de la SCSE, RO 2004, p. 5085, 5096.

13 Le Tribunal fédéral dit du reste explicitement au consid. 5.5 de l'arrêt que le fait qu'un courriel soit électroniquement signé est uniquement un problème de force probante du titre, mais que cela ne joue aucun rôle dans le fait qu'un courriel – signé ou non – puisse être propre ou destiné à prouver un élément.

14 Voir notamment le Règlement du Tribunal fédéral sur la communication électronique avec les parties et les autorités précédentes (RCETF, RS 173.110.29).

15 Voir l'annexe au RCETF. Par ailleurs, selon le site de la chancellerie fédérale, depuis le 1er juillet 2011, la plate-forme des données Open eGov Secure Inbox système pour l'administration fédérale (OSIS-BV), qui est gérée par l'entreprise fence IT AG pour l'OFJ, est provisoirement approuvée, voir http://www.bk.admin.ch/themen/egov/05755/index.html?lang=fr (consulté le 16 novembre 2013). Mais elle n'est pas ouverte de la même façon que les deux services précédents et n'est notamment pas valide pour la communication avec le Tribunal fédéral selon l'annexe au RCETF.

16 Voir http://www.incamail.ch ou https://im.post.ch (consultés le 16 novembre 2013).

17 Voir http://www.privasphere.ch (consulté le 16 novembre 2013).

1. Système d'expédition et de réception

L'expéditeur qui souhaite adresser un courriel recommandé par le biais d'INCAMail doit s'inscrire auprès de la Poste, ce qui peut se faire via un formulaire en ligne. Il pourra ensuite expédier un recommandé électronique. Lorsque le système INCAMail reçoit le courriel, il émet une quittance d'émission sous la forme d'un document PDF signé qui est adressée par courriel à l'émetteur.

Pour le destinataire, les choses sont théoriquement simples. Selon les instructions de la Poste, le destinataire d'un courriel recommandé reçoit un courriel signé électroniquement par la Poste l'informant qu'un message l'attend. Le destinataire doit alors explicitement indiquer s'il accepte ou refuse le recommandé, ce qui générera une seconde quittance électronique à l'intention de l'émetteur[18].

Malheureusement, la pratique est infiniment compliquée si le destinataire n'est pas lui-même inscrit pour l'utilisation du système INCAMail. Le destinataire devra d'abord ouvrir un compte INCAMail et faire vérifier son adresse électronique. Cela fait, il devra faire valider son adresse postale réelle, à moins qu'il fasse la preuve de son identité numérique via sa SuisseID. Le processus de validation est le suivant : le destinataire indique son adresse physique réelle dans le système. La Poste lui envoie alors par courrier ordinaire un code unique qu'il lui faudra saisir sur Internet dans son compte INCAMail à réception (quelques jours plus tard) pour prouver son identité. Ce n'est qu'à ce moment que le destinataire pourra décider s'il veut prendre connaissance du courriel recommandé et, cas échéant, le lire effectivement.

Le système concurrent mis en place par l'autre plate-forme reconnue, PrivaSphere, est *mutatis mutandis* identique s'agissant de l'expéditeur ; il est à peine moins compliqué pour le destinataire. Si celui-ci n'est pas préalablement identifié et enregistré, il ne pourra prendre connaissance du message qu'à la condition d'avoir saisi un code à usage unique que l'émetteur lui adressera séparément par télécopie, SMS ou oralement[19]. Le service propose même un courrier à télécopier au destinataire, indiquant en substance : cher destinataire, voici une télécopie qui vous permettra de vous connecter à votre navigateur web pour prendre connaissance du courriel que je vous ai envoyé[20].

---

18 Mode d'emploi du service IncaMail, page 9. Voir http://www.post.ch/fr/post-startseite/post-incamail-home/post-incamail-downloads.htm (consulté le 16 novembre 2013).

19 Voir conditions d'utilisation de PrivaSphere, disponibles en allemand et, suivant les sujets, en anglais, à l'adresse https://www.privasphere.com/hp/index.php ?id=59&L=1 (consulté le 16 novembre 2013).

20 D'aucuns ont peut-être pensé que la citation figurant en exergue de cet article et imputée à M. Bolomey, client inquiet n'était que le fruit de l'exagération emphatique d'un avocat...

Que l'on utilise INCAMail ou PrivaSphere, il est extrêmement probable que le système informatique du destinataire indiquera que la signature électronique est douteuse, pour les raisons techniques exposées ci-dessus.

Objectivement, les chances qu'un destinataire non enregistré préalablement prenne connaissance du courriel ne sont raisonnables qu'à la condition que le destinataire souhaite recevoir le courriel. Or, l'intérêt principal du courrier papier recommandé est de se ménager un moyen de preuve à l'égard d'un destinataire dont on soupçonne qu'il pourrait contester avoir reçu le message. Pratiquement, dès lors, espérer que le destinataire prendra connaissance contre son gré du message est une pure vue de l'esprit.

2. Conséquences juridiques de la (non-) réception

En matière de droit public, la jurisprudence a posé de longue date qu'il appartient à celui qui ne se trouve pas à son domicile de prendre ses dispositions pour recevoir malgré tout les communications qui lui sont adressées ou de désigner un tiers pour agir en son nom[21]. S'agissant du moment de la réception, les envois adressés par recommandé mais non retirés sont réputés notifiés le dernier jour du délai légal de garde[22], respectivement le dernier jour d'un délai de sept jours dès réception du pli par l'office postal du domicile du destinataire[23]. La jurisprudence du Tribunal fédéral établit à cet égard la présomption que l'employé postal a correctement inséré l'avis de retrait dans la boîte à lettres ou la case postale du destinataire et que la date de ce dépôt, telle qu'elle figure sur la liste des notifications, est exacte[24]. De même, les envois « poste restante » sont réputés notifiés au moment où ils sont retirés au bureau de poste ; si le retrait n'intervient pas pendant le délai de garde d'un mois, l'envoi est réputé notifié le dernier jour de ce délai[25]. Enfin, lorsqu'un acte est remis par porteur mais refusé et que le refus est constaté, c'est la date du refus qui est déterminante[26].

En matière de droit privé, la réponse à apporter est plus nuancée. De manière générale, en ce qui concerne une lettre recommandée, si l'agent postal n'a pas pu la remettre effectivement au destinataire ou à un tiers autorisé à prendre livraison de l'envoi et qu'il laisse

21 ATF 113 Ib 296, consid. 2a et les réf. Pour une référence récente, voir TF 9C_413/2011 du 15 mai 2012.

22 ATF 123 III 492.

23 ATF 134 V 49.

24 TF 1C_171/2011 du 26 mai 2011. Cette présomption est cependant réfragable ; s'agissant de prouver un fait négatif (soit qu'aucun avis n'a été déposé), une preuve stricte de l'absence de dépôt n'est pas nécessaire, la vraisemblance prépondérante suffisant (TF 2C_86/2010 du 4 octobre 2010, consid. 2.3 et les arrêts cités).

25 ATF 111 V 99.

26 Art. 138 CPC et 85 CPP.

un avis de retrait dans sa boîte aux lettres ou sa case postale, le pli est reçu dès que le destinataire est en mesure d'en prendre connaissance au bureau de la poste selon l'avis de retrait ; il s'agit soit du jour même où l'avis de retrait est déposé dans la boîte aux lettres si l'on peut attendre du destinataire qu'il le retire aussitôt, sinon en règle générale le lendemain de ce jour ; il s'agit là de la théorie de réception absolue[27]. Il y a cependant deux grandes exceptions à ce principe. D'une part, lorsque le destinataire est absent avec l'assentiment de l'expéditeur, ce dernier ne peut se prévaloir d'une notification avant le retour du destinataire. Ainsi, lorsque le travailleur prend des vacances avec l'accord de son employeur, une lettre de résiliation ne saurait être réputée reçue avant le retour de vacances[28]. D'autre part, dans certains cas où la protection très spécifique d'une partie exige qu'on lui accorde l'entier du délai prévu par la loi. Ainsi tant l'avis de majoration du loyer du locataire[29] que la menace de résiliation pour non-paiement du loyer[30] sont soumises à la théorie de la réception relative : l'acte n'est réputé retiré qu'au moment où le locataire en prend effectivement connaissance, mais au plus tard à l'expiration du délai de garde, comme pour les actes notifiés par une autorité[31].

a) Réception du message par son destinataire

Nous avons vu ci-dessus que les conditions de délivrance des signatures électroniques ont fait l'objet de normes précises fondées sur la SCSE. En revanche, le fonctionnement des plate-formes informatiques servant à expédier et recevoir des correspondances électroniques qualifiées (plate-formes de distribution) n'a pas été codifié par le législateur. Cela ne va pas sans poser des questions délicates.

Si le destinataire a accepté le message, celui-ci aura tous les effets d'un courrier signé dont il sera possible de prouver tant la réception que le contenu ; cela présente un léger avantage théorique par rapport au recommandé papier, puisqu'il est théoriquement relativement facile d'altérer la première page d'une correspondance dont seule la dernière est signée, alors que l'intégrité d'un document électroniquement signé peut être démontrée.

La date de réception dépendra du type d'acte. S'agissant d'une notification par le Tribunal fédéral, l'art. 7 du Règlement du Tribunal fédéral sur la communication électronique avec les parties et les autorités précédentes adopte un système équivalent à

27 ATF 137 III 208, consid. 3.1.3 ; ATF 107 II 189, consid. 2 et les réf.

28 TF 4P.307/1999 du 5 avril 2000 ; TF 4C.34/2006 du 4 mai 2006. En revanche, lorsque le travailleur prend ses vacances sans en informer son employeur, il redevient soumis aux règles ordinaires (TF 4P.307/1999, consid. 3c et les nombreuses réf. de doctrine).

29 ATF 107 II 189.

30 ATF 119 II 147, JdT 1994 I 205, SJ 1993 672 (rés.).

31 ATF 137 III 208.

celui qui prévaut en matière de courrier recommandé : c'est le moment où le destinataire télécharge la communication qui fait foi, mais au plus tard sept jours après le dépôt de cette communication sur la plate-forme de distribution. En ce qui concerne les actes notifiés par les autres autorités, la règle générale est que c'est la date de retrait effectif qui prévaut, sauf utilisation d'une boîte postale électronique sur une plate-forme reconnue, auquel cas s'appliquent les mêmes règles que pour les recommandés ordinaires en procédure civile ou pénale[32].

S'agissant enfin d'un courriel recommandé privé, la logique voudrait que c'est le moment où le recommandé est déposé dans la boîte électronique du destinataire qui fait foi, indépendamment de la date de retrait effective : les accès à une boîte électronique ne dépendent que d'une connexion Internet et non d'un déplacement physique du destinataire, de sorte que, même au bout du monde, chacun peut accéder quotidiennement à son compte[33]. Par analogie toutefois avec la jurisprudence, il nous paraît que le destinataire devrait pouvoir être admis à faire la preuve qu'il a été empêché sans sa faute de prendre connaissance du courriel recommandé, dans les limites du délai de garde toutefois.

b) Non-réception du message par son destinataire

Si le contenu du message ne parvient pas à son destinataire, se posera la question des conséquences de cette absence de prise de connaissance. Il faut distinguer selon les circonstances.

Lorsque le courriel est effectivement déposé dans une boîte électronique appartenant au destinataire[34], c'est en principe le moment du dépôt qui doit faire foi, pour les raisons exposées ci-dessus. Toutefois, nous envisagions des situations où le destinataire n'est pas en mesure de prendre connaissance du recommandé électronique. En cas de refus exprès du courriel, c'est alors au plus tard au moment du refus que le courriel sera réputé délivré : cette solution correspond à celle des articles 138 CPC et 85 CPP et ne diffère en rien de la situation du travailleur qui se voit remettre en main propre une résiliation de contrat mais refuse d'en prendre connaissance. En cas de non-consultation, c'est alors le délai de garde de sept jours qui doit s'appliquer, par analogie tant avec la jurisprudence rendue en matière de recommandé ordinaire qu'avec les normes applicables aux recommandés électroniques adressés par les tribunaux. A noter que l'exception admise par la doctrine et la jurisprudence en matière de vacances du travailleur ne devrait pas systéma-

32 Art. 138 CPC et 85 CPP applicables par renvoi de l'art. 11 OCEl-PCPP.

33 Solution du reste admise par le Tribunal cantonal des Grisons pour un courriel non recommandé, au motif que le courriel est parvenu dans la sphère d'influence du travailleur. Sur la question, voir BONARD, N 4 ad art. 335*d* CO.

34 Ce qui présuppose que le destinataire est effectivement inscrit sur la plate-forme de distribution.

tiquement trouver application, puisque la possibilité pour le travailleur d'accéder à ses courriels existe aujourd'hui quasiment dans le monde entier. Il va cependant de soi que si l'employeur a été informé que son employé part en trekking dans l'Himalaya ou entreprend une méditation dans le désert, il ne pourra pas compter que l'employé sera disponible pour réceptionner une communication.

Plus délicate est la situation du destinataire non inscrit sur une plate-forme de distribution. Comme nous l'avons exposé ci-dessus, la réception d'un courriel recommandé peut tenir du parcours du combattant. Nous avons tenté, au moyen du système INCAMail, de transmettre un courriel recommandé à un proche qui en était informé et a tout mis en oeuvre pour le lire le plus rapidement possible, mais la simple atteinte du code adressé par courrier ordinaire a retardé de plusieurs jours la prise de connaissance du message. De notre point de vue, dans de telles circonstances, on ne saurait contraindre une personne n'utilisant pas habituellement les communications électroniques qualifiées à accepter une telle communication. En d'autres termes, nous estimons que seule l'éventuelle réception effective par le destinataire, à l'exclusion de toute fiction, peut déclencher des conséquences juridiques[35].

En droit du travail, un moyen de contourner cette difficulté serait de subordonner l'engagement du travailleur à son inscription sur une plate-forme électronique qualifiée, ou d'imposer cette inscription aux travailleurs en fonction par le bais de l'art. 321*d* CO. On se trouve sans doute aux limites du pouvoir de l'employeur de donner des instructions, qui pourraient empiéter sur la vie privée de ses employés[36]. Supposé que les employés se soient pliés à cette exigence, la communication d'un licenciement ou d'une mise en demeure à un employé absent du travail pour des motifs douteux serait facilitée. En revanche, le refus du travailleur, par hypothèse injustifié, d'obéir à cette injonction ne pourrait guère entraîner un licenciement que par la voie d'une résiliation non électronique.

c) Synthèse

Entre particuliers, le courriel recommandé ne présente guère d'avantages. A son crédit pourra parfois être portée une fiction plus rapide de notification[37] et, en droit du travail,

35 A rapprocher des art. 86 CPP, 139 CPC et 9 OCEl-PCPP qui subordonnent le caractère contraignant des communications électroniques qualifiées à leur acceptation préalable par le destinataire.

36 Sur la question STREIFF/VON KAENEL/RUDOLF, N 3 ad art. 321*d* CO.

37 Pour autant que l'on n'adhère pas à la théorie selon laquelle même un courriel non signé est réputé réceptionné dès qu'il entre dans la sphère d'influence du destinataire comme l'admet le Tribunal cantonal grison (JAR 2007, p. 453).

la possibilité d'adresser un licenciement durant une période de vacances[38]. Mais la lourdeur et la complexité du système, tout comme l'obligation d'une inscription préalable à toute communication (ce qui n'est pas le cas du courrier ordinaire même recommandé), limite par trop l'intérêt de son usage.

II. SMS

Aucune réglementation spécifique n'a été édictée s'agissant du SMS. Faute de signature manuscrite, le SMS ne saurait être considéré comme un écrit ; par ailleurs, il n'existe pas d'infrastructure permettant de chiffrer et de signer un SMS, ce qui serait du reste techniquement difficile vu la limitation à 160 caractères.

Pourtant le SMS constitue un moyen de communication ordinaire et parfaitement valide lorsque la forme écrite n'est pas requise. Ainsi un avertissement en vue d'une résiliation, qui n'est soumis à aucune forme[39], pourra être signifié par SMS[40]. Il en va de même, pour des raisons identiques, de la résiliation[41]. Comme nous l'avons signalé ci-dessus, une décision grisonne, que nous approuvons, considère qu'un SMS, tout comme un courriel ou un fax, est réputé reçu non quand l'utilisateur en prend note mais lorsqu'il entre dans sa sphère d'influence, soit au moment où il est délivré au destinataire[42]. Il faudra malgré tout réserver le cas où le destinataire n'est pas en mesure de recevoir un SMS : ainsi, en fonction des conditions notamment du *roaming*, on pourra admettre que le possesseur d'un téléphone portable n'est pas en mesure de recevoir un SMS lorsqu'il se trouve à l'étranger. Il en ira de même en cas de perte ou de vol du téléphone : contrairement à une adresse physique forcément fixe qui permet à l'habitant de déléguer à un tiers le soin de relever sa boîte aux lettres, le SMS est en principe strictement limité à la carte SIM à laquelle le numéro est affecté, de sorte que la disparition du téléphone portable la contenant interdit la prise de connaissance.

Enfin, il pourra être difficile de prouver qu'un SMS a effectivement été délivré au destinataire, à moins qu'un relevé de télécommunications permette de le constater. L'inverse sera beaucoup moins difficile, dès lors que la présence d'un SMS sur un téléphone por-

38 Ce qui peut par ailleurs être obtenu par d'autres voies, voir ci-après.

39 TF 4A_170/2007 du 9 août 2007, consid. 4.1.

40 VÖGELI GALLI, p. 225.

41 STREIFF/VON KAENEL/RUDOLF, N 5 ad art. 335 CO; JAR 2007, p. 453 ; BONARD, N 6 ad art. 335 CO.

42 JAR 2007, p. 453. Sur la question, également STREIFF/VON KAENEL/RUDOLF, N 5 ad art. 335 CO ; GEISER/MÜLLER, N 591.

table constituera *a priori* la démonstration que le SMS a effectivement été envoyé par le détenteur du numéro figurant comme expéditeur[43]. Cela ne signifiera toutefois pas que le téléphone n'a pas pu être utilisé par un tiers[44] ; cela n'exclut enfin techniquement pas que la liste des SMS ait pu être modifiée par le récepteur, même si la plupart des utilisateurs ne disposent pas des connaissances suffisantes pour le faire[45].

Dans les relations de travail, une question mérite un commentaire particulier, celle de l'opposition au congé considéré comme abusif. A teneur de l'art. 336*a* CO, l'opposition doit être formée par écrit. Cela exclut théoriquement que l'opposition puisse être formée par SMS, faute que celui-ci soit muni d'une signature qualifiée au sens de l'art. 14 al. 2bis CO. Selon un *obiter dictum* d'une décision saint-galloise, il serait possible de faire opposition au congé par SMS[46]. Nous doutons que cette affirmation, par ailleurs non motivée, soit conforme au droit, tout en relevant que la question est controversée[47].

III. Informations officielles

Depuis le 1er janvier 2005, le registre du commerce existe sous une forme électronique en vertu de l'art. 929*a* CO. La version consultable sur Internet est cependant dénuée de portée juridique, seul faisant foi un extrait certifié conforme délivré par l'autorité.

Le législateur s'est préoccupé de cette situation. Un avant-projet de modification du Code des obligations circule à l'heure actuelle et vise à introduire notamment une réglementation spécifique sur les données électroniques. L'utilisation du registre du commerce informatisé deviendrait obligatoire et l'effet de publicité serait attaché à la publication sur Internet.

En quoi cette solution – à supposer qu'elle soit adoptée – changera-t-elle la pratique des particuliers et autorités ? Aujourd'hui, quand bien même la force publique n'est pas attachée aux inscriptions disponibles sur Internet, la pratique, à tout le moins des

43 Pour un exemple, voir arrêt TR07.033309-121208 du 19 septembre 2012 (cas de harcèlement sexuel essentiellement réalisé par l'envoi de SMS).

44 Cf. TF 4C.351/2004 du 20 janvier 2005 : licenciement avec effet immédiat fondé notamment sur les SMS expédiés du portable de l'employée mais non par elle.

45 http://minhdanh2002.blogspot.ch/2012/02/raw-access-to-sms-database-on-android.html (consulté le 16 novembre 2013).

46 JAR 2009, p. 568.

47 En faveur de la validité d'une opposition par e-mail non signé : PORTMANN, N 1*a* ad art. 336*b* CO. Contre cette interprétation STREIFF/VON KAENEL/RUDOLF, N 3 ad art. 336*b* CO ; dans le sens des précédents JAR 2011, p. 630.

autorités vaudoises, consiste à consulter Internet de manière systématique pour chaque dossier et à considérer comme probants les extraits ainsi obtenus[48]. Cette solution n'est au fond pas différente de celle adoptée par le Tribunal fédéral pour le courriel simple qui, tout en ne le considérant pas comme un titre, lui reconnaît un caractère probant complet.

La modification législative va dans le sens d'un caractère contraignant de l'électronique et complexifie une procédure aujourd'hui fort simple. Nous doutons que cette réglementation apporte sur ce plan un avantage majeur au justiciable.

IV. Stockage et l'archivage électroniques

Avec la généralisation des documents électroniques, la question de l'archivage a pris un tour différent. L'employeur qui doit stocker des archives, soit parce que cela a trait à ses pièces comptables, soit parce qu'il s'agit des données concernant son employé qu'il conserve au sens de l'art. 328*b* CO, a un intérêt évident à ce que les données soient stockées sous forme immatérielle plutôt que sous forme de documents dans des armoires.

A. Avantages de l'électronique

Les avantages du stockage électronique sont de deux sortes. D'une part, un document numérisé prend infiniment moins de place qu'un document papier. La quantité d'informations qu'il est possible de stocker dans une carte de type Micro SD présente dans de nombreux smartphones est à ce jour de 64 Go pour 158 mm^3, soit une densité d'information de quelque 405 Go par cm^3 ou 405 Po par m^3 [49]. Avec une taille de stockage de l'ordre de 10 Ko par page pour un document texte ou de 1 Mo par image, le mètre cube de donnée pourrait contenir l'équivalent de plusieurs centaines de milliards d'images ou de plusieurs dizaines de milliers de milliards de pages de texte, soit largement de quoi dépasser la quantité de documents qu'une personne peut produire en une vie.

D'autre part un document électronique peut être copié en un temps très court. Les taux de transfert des supports de stockage comme des câbles les reliant entre eux est à ce jour de l'ordre de quelques dizaines, voire quelques centaines de Mo par seconde. La prise d'une copie complète d'un support de données contenant plusieurs millions de docu-

48 Nous nous y sommes mis de manière définitive le jour où nous avons commandé un extrait papier pour une inscription qui avait été modifiée entre le jour d'émission de l'extrait et sa réception postale.

49 Voir http://fr.wikipedia.org/wiki/Carte_microSD (consulté le 16 novembre 2013).

ments ne représente que quelques minutes, de sorte qu'il est très facile de réaliser une sauvegarde complète des données d'une entreprise.

B. Inconvénients de l'électronique

Aux avantages exposés ci-dessus correspondent un certain nombre d'inconvénients et de risques. Dans une précédente publication[50], nous avions rappelé certains des risques spécifiques aux documents électroniques : multiplication aisée des documents, avec un risque de dispersion et de perte de maîtrise, grande difficulté à assurer qu'un document électronique a été effectivement détruit, le seul effacement du fichier sur le disque dur étant à cet égard largement insuffisant, risque d'altération ou de perte de données en raison de virus informatiques, transmission de données à l'insu de l'émetteur, notamment en raison de l'enregistrement pas toujours maîtrisé dans un document d'informations relatives à des versions antérieures, etc. Ces risques n'ont pas ou peu évolué depuis.

Nous présentons ci-après deux problématiques supplémentaires particulièrement importantes pour l'entreprise : la notion d'authenticité des données dans la conservation des archives et la protection des données lors de leur enregistrement sur des infrastructures externes aux locaux de l'entreprise.

1. Conservation et authenticité des données

Deux normes spécifiques régissent la conservation de documents par l'employeur : les art. 328*b* et 58*f* CO.

S'agissant du traitement de données relatives aux employés, l'art. 328*b* CO pose essentiellement les limites au traitement et déclare la Loi sur la protection des données[51] applicable. Selon l'art. 7 LPD, les données personnelles doivent être protégées contre tout traitement non autorisé par des mesures organisationnelles et techniques appropriées. La liste des mesures à prendre, concrétisée aux art. 8 et 9 OLPD[52], contient notamment la protection contre les risques de destruction accidentelle ou non autorisée, de perte accidentelle, d'erreurs techniques, de falsification, vol ou utilisation illicite et de modification, copie, accès ou autre traitement non autorisés.

Si certaines mesures sont relativement évidentes[53] (sauvegardes périodiques, protection par mots de passe notamment), d'autres le sont moins, notamment en ce qui a trait aux

---

50 SUBILIA, p. 50 ss.

51 Loi fédérale du 19 juin 1992 sur la protection des données (LPD, RS 235.1).

52 Ordonnance du 14 juin 1993 relative à la Loi fédérale sur la protection des données, RS 235.11.

53 Sur l'ensemble des mesures à prendre en matière de communication électronique, voir FAVRE.

risques de falsification des données. Il n'existe guère qu'un moyen d'assurer l'intégrité d'un document électronique : la signature du document. Faut-il donc considérer que le stockage de documents électroniques est conditionné à l'utilisation d'un chiffrement pour qu'il soit considéré comme suffisamment protégé ? Nous ne le pensons pas, car le risque de modification d'un document se confond avec le risque de destruction du même document et dépend des possibilités d'accès par des tiers non autorisés. Si l'on admet – ce que nous pensons – qu'un système de protection par mot de passe est suffisant pour garantir la sécurité des accès, la limitation du risque de falsification doit être considérée comme assurée au niveau de l'accès aux données également[54].

En matière de comptabilité, la situation est un peu différente. Alors que l'art. 958*f* al. 3 CO prévoit expressément toutes sortes de supports, papier, électronique ou autres[55], l'alinéa 2 de cette même disposition impose la conservation d'un document imprimé et signé s'agissant des rapports de gestion et de révision. Bien que le texte ne l'exige pas expressément, le Message précise que les livres et pièces comptables doivent être pourvus d'une signature électronique qualifiée s'ils sont conservés sous une forme informatique[56]. Cela découle en réalité de la formulation de l'art. 957*a* qui définit la pièce comptable comme tout document *écrit* établi soit sur papier, soit sous forme électronique. L'écrit suppose ainsi une signature qualifiée.

Lorsque les documents auront été établis directement sous forme électronique, leur préparation en vue du stockage ne posera pas de problème particulier. En revanche, s'il s'agit de remplacer les documents papier par des documents informatiques, il sera nécessaire d'adjoindre une signature électronique certifiée aux documents numérisés pour qu'ils satisfassent aux exigences légales[57].

2. Problème de protection des données

La protection des données pose en matière de stockage et d'archivage électronique des problèmes qui ne se posent pas avec des documents papier. En effet, si le lieu de stockage d'un document physique est immédiatement déterminable, celui d'un document électronique ne l'est pas toujours. Un document électronique se trouve « physiquement » sur le support matériel de donnée sur lequel il a été enregistré. Si l'on enregistre un

54 Le Préposé fédéral à la protection des données ne recommande pas officiellement l'usage d'une signature qualifiée pour le stockage de toute pièce. Voir http://www.leprepose.ch, rubrique internet et ordinateur / sécurité des données (consulté le 16 novembre 2013).

55 On se demande quel pourrait être cet autre, que le Message ne qualifie pas. L'art. 9 de l'Ordonnance du 24 avril 2002 concernant la tenue et la conservation des livres de comptes (Olico, RS 221.431) n'apporte pas davantage de précisions.

56 FF 2008 1407, p. 1523.

57 Par exemple sous forme de PDF signés.

document sur un support local (disque dur de l'ordinateur, par exemple), le document est à proximité. En revanche, si l'on sauvegarde les données sur un support réseau (disque dur partagé, *cloud computing*, service de stockage distant, etc.), le lieu où se trouvent les données n'est pas forcément apparent.

Si le lieu de stockage, en tout ou partie, est à l'étranger, l'on est alors en présence d'un traitement transfrontière des données au sens de l'art. 6 LPD. En effet, même si la personne qui, de son bureau, enregistre un document n'a pas l'impression de « communiquer » des données à l'étranger, elle les transfère malgré tout sur un support de données situé hors du territoire suisse[58]. L'article 6 LPD dispose : « *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* »[59]. En d'autre termes, celui qui, consciemment ou non, stocke des données à l'étranger ne peut le faire sans s'assurer du type de protection offert dans le pays d'hébergement[60].

La situation dépend essentiellement du pays de destination. Le protocole additionnel à la convention STE n° 108[61] oblige les différentes parties à prévoir que le transfert de données à caractère personnel vers un destinataire soumis à la juridiction d'un Etat ou d'une organisation qui ne fait pas partie à la Convention STE n° 108 ne peut être effectué que si ces Etats ou cette organisation assure un niveau de protection adéquat pour le transfert considéré (article 2 § 1). *A contrario*, la convention STE n° 108 garantit une certaine circulation internationale des données, en ce sens qu'aucun Etat partie ne peut interdire le transfert d'information vers un autre Etat partie qui accorde la protection minimale qu'elle prévoit et présume ainsi que la protection apportée par les pays signataires est suffisante[62]. On trouvera sur le site du Préposé fédéral à la protection des données[63] la liste des pays dont la législation est réputée offrir des garanties suffisantes

58 Voir STREIFF/VON KAENEL/RUDOLF, N 10*b* ad art. 328*b* CO ; MEIER, N 1269.

59 Cette disposition a été assez profondément remaniée avec effet au 1er janvier 2008, et a été adaptée à la convention du Conseil de l'Europe sur la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (convention STE n° 108, RS 0.235.1) et à son protocole additionnel.

60 MEIER, N 1286 ss.

61 Signé par le Conseil fédéral et ratifié le 20 janvier 2007 ; RS 0.235.11.

62 Voir MEIER, N 1296 et les réf.

63 http://www.leprepose.ch (consulté le 16 novembre 2013).

au sens de l'art. 6 LPD[64]. Les Etats-Unis n'en font pas partie, du moins pas sans conditions, ce à quoi les employeurs avec une activité internationale devraient être attentifs.

V. Communications avec les autorités

En matière de communication avec les autorités, le législateur fédéral mais surtout le Conseil fédéral et le Tribunal fédéral ont mis en place des règles nettement plus contraignantes que celles qui s'appliquent aux communications entre particuliers.

A. Procédure cantonale

Les principes régissant la communication avec les autorités en matière civile, pénale et de poursuites pour dettes sont fixés dans l'OCEl-PCPP[65]. Ce texte détermine des principes généraux tout en laissant aux cantons toute latitude pour la mise en oeuvre de ces principes, y compris pour ne pas les mettre en oeuvre[66].

Une comparaison des différentes législations cantonales dépasserait le cadre de cette étude. Nous ne mentionnons ainsi ce texte que pour mémoire.

B. Recours devant le Tribunal fédéral

Depuis le 1er janvier 2007, il est possible de déposer des recours par voie électronique. Cette nouveauté a été introduite par la LTF, le législateur constatant que la jurisprudence du Tribunal fédéral notamment en matière de télécopie[67] – le Tribunal fédéral, nonobstant l'ancien art. 30 al. 2 OJ qui prévoyait de ratifier postérieurement un recours non signé lors de l'envoi, estimait que celui qui expédiait un recours par télécopie (soit un acte non signé selon la jurisprudence) omettait délibérément sa signature ce qui lui interdisait de réparer ultérieurement le vice – faisait obstacle *de lege lata* à toute reconnaissance de validité d'un acte déposé sous forme électronique.

---

64 Quand bien même cette liste ne lie théoriquement pas le juge civil, on voit mal que l'on exige du particulier un examen plus attentif que celui du Préposé fédéral à la protection des données. Voir MEIER, N 1307.

65 Ordonnance du 18 juin 2010 sur la communication électronique dans le cadre de procédures civiles et pénales et de procédures en matière de poursuite pour dettes et de faillite, RS 272.1.

66 Voir ci-après.

67 ATF 121 II 252.

Le système adopté par le législateur fédéral n'est cependant pas des plus simples. Les Messages relatifs à la révision totale de l'organisation judiciaire fédérale[68] du 28 février 2001 et à la Loi fédérale sur les services de certification dans le domaine de la signature électronique[69] du 3 juillet 2001 étaient quasiment simultanés. Dès lors que la jurisprudence admet que les principes de forme posés par les art. 11 ss CO valent également pour les actes unilatéraux[70] et que le nouvel art. 14 al. 2bis CO était également en gestation, on aurait pu imaginer que la signature électronique apposée sur n'importe quel document électronique suffise. En réalité, les différences entre la procédure ordinaire et la procédure électronique sont importantes et les normes sont nettement plus contraignantes dans le second cas.

1. Problèmes généraux de forme

Selon l'art. 42 al. 1 LTF, les mémoires doivent être rédigés dans une langue officielle, indiquer les conclusions, les motifs et les moyens de preuve et être signés. Aucune prescription n'a en revanche été édictée en matière de format de document. Un recours peut ainsi être manuscrit ou dactylographié pourvu qu'il comporte une signature manuscrite. Il peut être soumis en format A4 ou sous n'importe quelle autre forme, la seule réserve étant que l'acte ne doit être ni inconvenant ni illisible (art. 42 al. 6 LTF). Les pièces peuvent être remises sous forme de photocopies.

L'art. 42 al. 4 LTF introduit la possibilité pour le Tribunal fédéral de mettre des conditions spécifiques de forme pour les documents électroniques. Selon l'art. 4 RCETF, les parties adressent leurs mémoires au Tribunal fédéral en format PDF accompagné d'un fichier XML et les annexes en format PDF. Elles utilisent à cet effet les formulaires mis à disposition par le Tribunal fédéral sur son site Internet ou sur la plate-forme de distribution.

Concrètement, cela signifie que le format du document est imposé, tout comme l'utilisation d'un logiciel propriétaire, soit Adobe Acrobat Reader. Le Tribunal fédéral met à disposition son propre document à compléter, ne fonctionnant qu'avec ce logiciel[71]. Il n'est pas possible de signer seulement le message contenant tous les documents mais chaque document doit être signé séparément, ce qui oblige – au prix de diffi-

68 FF 2001 4000.

69 FF 2001 1276.

70 Voir notamment ATF 121 III 31, JdT 1997 II 105, dans lequel le Tribunal fédéral applique l'art. 11 CO pour déterminer la notion de forme dans la LPP (de droit public).

71 L'utilisation des logiciels Okular ou Display/ImageMagick, par exemple, ne donne que la phrase suivante : « *If this message is not eventually replaced by the proper contents of the document, your PDF viewer may not be able to display this type of document* » et renvoie vers le site d'Adobe.

cultés informatiques parfois significatives – à utiliser le système de signature propre à Acrobat Reader.

2. Nécessité d'une inscription

Tout un chacun peut adresser un recours au Tribunal fédéral, pour autant que le recours soit rédigé en format papier. L'utilisation de la voie électronique suppose en revanche que l'on se soit préalablement inscrit sur une plate-forme de distribution électronique reconnue (art. 3 al. 1 RCETF). Par ailleurs, cette inscription oblige automatiquement la personne inscrite à accepter qu'on lui adresse à son tour n'importe quel acte de procédure sous la forme de documents électroniques (art. 3 al. 2 RCETF, règle qui nous paraît contrevenir à la volonté clairement exprimée par le législateur de laisser la liberté au justiciable d'accepter ou non la seule notification[72]).

3. Utilisation obligatoire d'une transmission « recommandée » et transfert des risques

Pour être déposé en temps utile, un recours en format papier doit simplement être remis soit directement au Tribunal fédéral, soit à un bureau de poste suisse (art. 48 al. 1 LTF). Le choix d'utiliser la forme simple ou la forme recommandée appartient au justiciable ; en particulier, la loi n'impose aucunement le recours à l'envoi recommandé, quand bien même celui-ci offre en matière de preuve d'indéniables facilités pour l'expéditeur[73].

Par ailleurs, le justiciable peut se prémunir contre toute défaillance dans le système d'acheminement des documents par voie postale. S'il ne trouve pas de bureau de poste ouvert, il pourra alors déposer son recours dans une simple boîte aux lettres en veillant à disposer d'une personne tierce pouvant attester de la date et de l'heure de la remise[74]. Un témoin permettra même de renverser la présomption d'exactitude que revêt le sceau postal apposé sur l'enveloppe[75].

Enfin, si l'autorité ne reçoit jamais l'acte, celui-ci n'en aura pas moins été réputé déposé dans le délai imparti s'il a été mis dans une boîte aux lettres en temps utile[76].

En revanche, le respect des délais par la voie électronique suppose obligatoirement l'obtention d'un accusé de réception d'une plate-forme spécifique (art. 48 al. 3 LTF). Bien que le recours s'exerce par écrit et que l'article 14 al. 2bis CO assimile purement et

72 Art. 39 LTF ; voir également FF 2001 4000, p. 4091.
73 Voir TF 2C_404/2011 du 21 novembre 2011.
74 ATF 97 III 12 et les nombreuses réf.
75 Voir par exemple TF 5A_267/2008 du 16 octobre 2008.
76 Entre autres ATF 97 III 12.

simplement le courrier électronique muni d'une signature qualifiée à un écrit, le Tribunal fédéral a confirmé que cette disposition n'était pas applicable aux actes judiciaires[77]. Il s'agissait d'un avocat bernois souhaitant déposer un recours par voie électronique dans son canton qui n'avait – à l'époque du moins – pas mis en place de plate-forme de communication électronique pour les tribunaux. Fondé sur l'art. 14 al. 2bis CO, l'avocat avait adressé au tribunal un recours par voie de courrier électronique « simple » mais muni d'une signature qualifiée. Non seulement la Haute Cour a confirmé qu'un tel recours n'était pas valable parce que non conforme à l'art. 4 OCEl-PCPP, quand bien même elle admettait qu'on ne comprenait guère pourquoi le canton n'avait pas mis en place la plate-forme légalement imposée, mais elle a refusé au recourant le droit de corriger sa procédure en adressant ultérieurement une version papier du même document : hors des formes prévues, un recours électronique n'a aucun effet s'agissant du respect des délais, de sorte qu'aucune guérison ultérieure n'est possible[78].

Enfin, la procédure en matière de recours électronique implique un transfert des risques important pour le justiciable. Alors que pour le format papier, c'est l'expédition qui fait foi, un recours électronique n'est réputé déposé qu'au moment où la réception de l'acte électronique est effectivement confirmée par la plate-forme utilisée par l'autorité. Selon le Tribunal fédéral, « en cas de transmission par voie électronique, l'observation ou non du délai se détermine non pas, comme dans les autres cas, en fonction de la date et de l'heure d'envoi, mais en fonction de la date et l'heure de confirmation de la réception de l'envoi par le système informatique de l'autorité pénale. Si la partie ne reçoit pas confirmation de la réception, elle doit mettre son pli à la poste encore dans le délai. Cela signifie que la partie qui utilise la voie électronique ne pourra guère prendre le risque d'envoyer l'écrit à minuit, voire quelques minutes avant, n'ayant pas la garantie que le système informatique répondra dans la minute ou la seconde qui suit »[79].

Le Tribunal fédéral a au moins admis que lorsque la plate-forme désignée[80] avait confirmé la réception du recours, le délai était sauvegardé, quand bien même l'autorité ne prenait connaissance du recours qu'ultérieurement. Le Tribunal fédéral distingue

77 TF 5A_650/2011du 27 janvier 2012.

78 La question de la guérison n'est qu'effleurée par le Tribunal fédéral, qui relève que le recourant ne conteste pas ce point de vue spécifique et examine la question davantage sous l'angle du formalisme excessif (nié en l'espèce). Au vu toutefois de la jurisprudence rendue en matière de recours adressé par télécopie (voir *supra*), il est vraisemblable que la guérison ultérieure n'aurait pas été admise, le recours ayant été volontairement adressé par voie électronique.

79 TF 6B_691/2012 du 21 février 2013.

80 En l'espèce, IncaMail.

ainsi, en matière de recours électronique, le dépôt dans la « case postale » électronique du destinataire et le relevé de la case en question[81].

Ce système est pratiquement identique à celui qui prévalait en matière de délais de paiement d'avances de frais sous l'empire de l'OJ. Lorsque le paiement était effectué par le débit d'un compte postal, le débit du compte suffisait au respect du délai. En revanche, lorsque le paiement était effectué par le débit d'un compte bancaire, c'est le paiement effectif sur le compte postal du Tribunal, ou à tout le moins la remise effective par la banque de l'ordre de transfert groupé à la Poste, qui comptait pour le respect du délai[82]. Ce système a été modifié lors de l'introduction de la LTF, en réponse à une motion parlementaire[83] observant que la réglementation datant de 1943 n'était plus adaptée à l'évolution des modes de paiement et faisait subir au justiciable de façon « choquante » les conséquences « de problèmes informatiques »[84].

Force est de constater qu'aujourd'hui, après l'adoption d'une nouvelle réglementation de rang légal destinée à éviter cette situation pour les délais d'avance de frais effectués par voie électronique[85], le Tribunal fédéral réintroduit par voie d'ordonnance un désavantage pour celui qui fait usage des moyens électroniques de communication. Nous doutons assez sérieusement que cette ordonnance corresponde véritablement à l'intention initiale du législateur, quand bien même sur le plan de la délégation de compétence le Tribunal fédéral a été formellement autorisé à adopter cette réglementation[86].

4. Emploi du recours électronique dans la pratique

Les conséquences pratiques de cette réglementation se manifestent on ne peut plus clairement dans l'absence presque totale d'utilisation de ce moyen. Selon le Tribunal fédéral lui-même[87], ont été déposés depuis l'introduction du système les recours suivants :

81 TF 1B_222/2013 du 19 juillet 2013.

82 ATF 118 Ia 8, JdT 1993 I 580 ; ATF 117 Ib 220, et les réf., JdT 1993 I 580.

83 Motion HANS HESS du 20.9.2000, n° 00.3446.

84 Voir texte de la motion sur www.parlement.ch (consulté le 16 novembre 2013).

85 FF 2001 4000, p. 4096 s.

86 Le Règlement du Tribunal fédéral sur la communication électronique avec les parties et les autorités précédentes est fondé sur les articles 42 al. 4 (expédition par les parties) et 60 al. 3 (communication aux parties) LTF, deux dispositions qui laissent toute latitude au Tribunal fédéral de fixer le cadre formel.

87 Informations disponibles sur le site du Tribunal fédéral, http://www.bger.ch (consulté le 16 novembre 2013).

– 1 sur 7'189 en 2009, soit 0,01% ;
– 3 sur 7'367 en 2010, soit 0,04% ;
- 20 sur 7'419 en 2011, soit 0,26% ;
- 25 sur 7'871 en 2012, soit 0,31%.

Mieux que n'importe quelle explication théorique, ces chiffres démontrent le caractère inutilisable du système.

VI. Conclusion

La communication électronique présente de multiples avantages dont la rapidité et la simplicité. Ces avantages ont conduit à leur adoption aujourd'hui à large échelle et leur usage se retrouve dans l'immense majorité des foyers, des entreprises et des situations de la vie quotidienne.

En comparaison, les normes légales régissant de façon spécifique la communication électronique sont lourdes, complexes et mal pratiques. L'usage de l'électronique sous sa forme qualifiée n'est de loin pas adapté à toutes les situations du droit. Que ce soit parce que le destinataire ne peut pas en faire usage de façon suffisamment pratique (certificat de travail[88]), voire ne donne pas son accord[89], ou parce que le média n'est pas compatible avec une signature électronique (mention manuscrite du montant de la garantie dans l'acte de cautionnement au sens de l'art. 493 al. 2 CO, testament olographe au sens de l'art. 55 CC[90]), le document électronique ne peut remplacer le papier. Quant à la lourdeur des procédures judiciaires numériques, elle a de quoi décourager les plus progressistes des acteurs du monde judiciaire.

Parallèlement à l'édiction des normes sur l'électronique qualifiée, la communication électronique simple se voit progressivement reconnue par la doctrine et la jurisprudence, notamment en matière de preuves.

En synthèse, nous estimons que – à l'heure actuelle à tout le moins – le recours à la communication électronique est utile et précieux, sauf dans les cas où son usage est spécifiquement régi par la législation suisse.

---

88 Voir SUBILIA, p. 47. Voir par analogie les considérations du Conseil fédéral pour qui on ne saurait, en matière de vote des actionnaires, contraindre les sociétés à accepter une procuration électronique alors même que la procuration électronique répond pleinement aux exigences de forme posées par le Code des obligations (FF 2008 1407, p. 1485).

89 Voir HURNI/WIEGAND, N 9 ad art. 14 CO.

90 Sur ces deux questions, voir FF 2001 5450.

VII. Bibliographie sommaire

BONARD ALINE, in : DUNAND/MAHON (édit.), Commentaire du contrat de travail, Berne 2013.

FAVRE KATIA, Sorgfaltspflichten bei der Datenübertragung, Zurich 2006.

GEISER/MÜLLER, Arbeitsrecht in der Schweiz, Berne 2009.

HURNI/WIEGAND, in : HONSELL (édit.), Obligationenrecht, Kurzkommentar, Bâle 2008.

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

STREIFF/VON KAENEL/RUDOLF, Arbeitsvertrag, Praxiskommentar zu Art. 319-362 OR, 7e éd., Zurich 2012.

SUBILIA OLIVIER, La relation de travail : quelques questions pratiques, in : Internet au lieu de travail, Travaux de la journée d'étude organisée à l'Université de Lausanne le 12 mai 2004.

VÖGELI GALLI NICOLE, Ablaufdatum einer Verwarnung, Revue de l'avocat 2013, p. 223.

WYLER RÉMY, Droit du travail, 2e éd., Berne 2008.

XOUDIS JULIA, in : THEVENOZ/WERRO (édit.), Commentaire romand, Code des obligations, Bâle 2012.