CERT

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

CERT
Centre d'étude
des relations de travail

unine
UNIVERSITÉ DE NEUCHÂTEL
FACULTÉ DE DROIT

Schulthess
ÉDITIONS ROMANDES

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

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

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.