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.