CERT

Jean-Philippe Dunand | Pascal Mahon (éd.)

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

Internet au travail

Préface de Laurent Kurth
Président du Conseil d'Etat neuchâtelois

CERT
Centre d'étude
des relations de travail

unine
UNIVERSITÉ DE NEUCHÂTEL
FACULTÉ DE DROIT

Schulthess
ÉDITIONS ROMANDES

Jean-Philippe Dunand | Pascal Mahon (éd.)

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

Internet au travail

Préface de Laurent Kurth
Président du Conseil d'Etat neuchâtelois

Centre d'étude des relations de travail

Schulthess
ÉDITIONS ROMANDES
§ 2014

Information bibliographique de la Deutsche Nationalbibliothek

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

ISBN 978-3-7255-6991-5

www.schulthess.com

Table des matières

Première partie - Cadre général et principes

Deuxième partie - Questions choisies

BERTIL COTTIER*

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

Sommaire Page

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

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

A. Introduction

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

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

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

---

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

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

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

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

B. Le silence des instances internationales

1. L'absence de texte topique contraignant

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

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

---

3 Cf. *infra* E.

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

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

2. Les raisons de ce silence

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

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

---

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

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

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

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

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

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

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

3. Les instruments cadre sur la protection des données

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

---

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

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

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

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

13 RS 0.235.1.

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

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

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

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

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

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

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

4. Et la *soft law* internationale ?

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

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

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

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

15 Cf. *infra* C.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

---

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

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

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

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

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

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

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

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

C. Les réponses nationales

1. Les lois sur la protection des données

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

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

---

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

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

30 *Codice* art. 114.

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

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

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

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

---

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

D. Un bouquet de jurisprudences européennes hétéroclites

1. Généralités

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

40 *Ibidem*, p. 15 ss.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

49 Cour de cassation, 2 octobre 2001.

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

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

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

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

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

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

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

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

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

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

---

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

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

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

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

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

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

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

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

F. Conclusion

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

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

---

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

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

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

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

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

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

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

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

II. Bibliographie

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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