Les communications électroniques et la protection de la vie privée sur le lieu de travail

Rosier, Karen

Published in:
L'Europe des droits de l'homme à l'heure d'Internet

Publication date:
2019

Document Version
le PDF de l'éditeur

CHAPITRE 11. LES COMMUNICATIONS ÉLECTRONIQUES ET LA PROTECTION DE LA VIE PRIVÉE SUR LE LIEU DE TRAVAIL

Karen ROSIER
Maître de conférences à l'UNamur
Avocate (Versius)

I. Propos introductifs

1. Il y a 25 ans, la Cour européenne des droits de l'homme affirmait le principe selon lequel le simple fait que l'on se trouve dans le contexte d'une vie professionnelle n'empêchait pas qu'un travailleur puisse se prévaloir de son droit au respect de la vie privée[1]. Elle allait même plus loin en soulignant que « [l]e 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 »[2]. Cette réalité reste plus que jamais d'actualité, en particulier dans le contexte des communications électroniques.

2. L'usage des technologies de communication amène à de nouveaux arbitrages à réaliser et le moins que l'on puisse dire est que la problématique de la conciliation entre le respect du droit à une vie privée dans le contexte des relations de travail et les spécificités liées à l'exercice de l'autorité patronale et à la vie économique de l'entreprise est éminemment complexe. Plusieurs facteurs nous semblent participer à cette complexité.

1 Cour eur. D.H., 16 décembre 1992, req. n° 13710/88, *Niemietz c. Allemagne*, § 29.
2 *Ibid.*

3. Tout d'abord, le développement de nouveaux moyens de communications va de pair avec de nouvelles pratiques. L'usage du courrier électronique et, plus récemment, de messageries instantanées a induit un mode d'expression plus spontané. Il n'est plus rare que des messages échangés dans un contexte professionnel prennent une teinte qui ne l'est plus exclusivement, professionnelle. On écrit à ses collègues, à un contact commercial de manière moins formelle, n'hésitant peut-être plus à ponctuer un propos professionnel de considérations liées à un autre contexte, voire même à inclure une émoticône que l'on n'aurait jamais eu l'audace d'intégrer dans courrier postal ou dans un fax. Ces nouveaux canaux de communication ont sans doute capté une série d'échanges qui se faisaient auparavant sans rémanence, au gré d'une discussion de vive voix. Il y a donc à notre sens à la fois une inflation des communications et une diversité du type de communication qui rend peu à peu obsolète l'idée que l'on pourrait classer des communications en deux catégories bien étanches : privées ou professionnelles. Dans le prolongement de cette idée, on peut se demander s'il n'est pas illusoire de prétendre exclure *a priori* toute dimension privée à ces communications, même dans un usage professionnel lié au fonctionnement de l'entreprise. Pourtant, ces communications, même plus informelles, font partie du patrimoine informationnel de l'entreprise et on conçoit mal que cette dernière ne puisse, en raison d'une protection du travailleur, les conserver, en prendre en connaissance ou encore les produire alors que cela s'avèrerait nécessaire au déroulement de ses activités.

4. Un deuxième facteur de complexité est la diversité des outils de communication et des aspects techniques qui les caractérise. Cette diversité concerne tant les moyens de communication (Internet, *e-mail*, services de messagerie *online*, téléphones, etc.) que les modes de stockage d'informations sur différents supports (PC, PC portables, tablettes, serveur *cloud*, etc.), ou encore les données générées et elle influe sur la maîtrise de ces données (données stockées sur un serveur de l'entreprise, sur un PC appartenant au travailleur selon la pratique du « *bring your own device* », par exemple).

Nous y reviendrons mais nous verrons que, selon le type d'outil utilisé, les moyens de contrôle peuvent se trouver restreints par des questions d'ordre technique ou juridique. En effet, dès lors qu'il s'agit de contrôler des communications protégées par le secret des communications électroniques cela devrait, nous semble-t-il mobiliser des règles plus strictes

que celles qui s'appliquent, par exemple, au contrôle de fichiers enregistrés sur un disque dur.

5. Un troisième aspect de la problématique qui nous semble d'ailleurs être des plus emblématiques au vu des derniers développements de la jurisprudence de la Cour européenne des droits de l'homme en matière de contrôle des communications électroniques, est la question de l'incidence de la politique de l'employeur. Il peut exister des pratiques très différentes d'une entreprise à l'autre concernant la culture de l'usage des technologies de sorte que ce qui pourrait parfaitement admis au sein d'une entreprise pourrait être interdit, et même sujet à sanction, dans une autre. Ainsi en est-il de l'usage de l'utilisation d'Internet, d'une boîte de messagerie professionnelle ou encore des réseaux sociaux comme canal de communication.

L'essence même de la relation de travail requiert la possibilité pour l'employeur d'exercer une autorité sur le travailleur, ce qui inclut la prérogative de lui donner des instructions sur l'utilisation des outils de travail mis à sa disposition. Pourrait-il pour autant interdire tout usage « privé » de ce matériel pour se ménager le droit de contrôler sans entrave ? Qu'en est-il éventuellement d'étendre cette interdiction à des outils appartenant au travailleur ? Nous verrons que le caractère essentiel de cette question se révèle particulièrement dans les deux décisions de la Cour européenne des droits de l'homme dans une affaire *Bărbulescu* et que nous commenterons sous la section II A, *infra*.

En tout état de cause, il n'y a pas de standards généraux et l'appréciation au cas par cas est particulièrement indiquée à cette problématique mais est également source d'insécurité juridique.

6. Nous identifierons, dans le cadre de la présente contribution, trois angles de protection du point de vue du droit européen qui ont tous en commun d'être des règlementations transversales, non spécifiques à la relation de travail.

Il s'agit du droit au respect de la vie privée (II), du droit à la protection des données à caractère personnel (III) et de la règlementation spécifique aux traitements de données liées aux communications électroniques (IV). Bien que certains principes qui gouvernent la mise en œuvre de ces droits peuvent paraître assez proches, nous verrons que le régime juridique propre à chaque protection implique des contraintes spécifiques qui, il est vrai, ne sont pas toujours évidentes à concilier avec les particularités du contexte de la relation de travail.

II. Le droit au respect de la vie privée

7. Les communications électroniques sont protégées en tant qu'elles relèvent du droit au respect de la vie privée et de la correspondance, et ce même dans un contexte professionnel. Ce droit fondamental est consacré de longue date par l'article 8 de la Convention européenne et a également été repris à l'article 7 de la Charte des droits fondamentaux de l'Union européenne. Nous ne reviendrons par sur les textes de ces dispositions qui sont largement commentés par ailleurs au sein du présent ouvrage, mais nous pencherons sur son application par la Cour européenne des droits de l'homme dans le contexte du contrôle ponctuel ou de la surveillance des communications électroniques dans la relation de travail.

A. – *La notion d'ingérence dans la vie privée*

8. Cette notion est première et fondamentale dans ce qui permet de considérer les contours de la protection de l'article 8 de la CEDH.

Elle comporte deux volets : celui de la notion de vie privée et celui d'ingérence.

Nous n'avons pas la prétention, dans le cadre de la présente contribution, de procéder à une analyse exhaustive de la jurisprudence de la Cour sur la question. Nous nous limiterons aux décisions touchant plus précisément au contrôle des communications électroniques (qui recouvrent les courriers électroniques, du téléphone et Internet, notamment).

Les deux premiers arrêts rendus ce domaine, à savoir les affaires ayant opposé respectivement Mmes Halford[3] et Copland[4] au Royaume-Uni, ont permis à la Cour de poser des jalons importants dans ce domaine. Ainsi, la Cour a-t-elle considéré que les appels téléphoniques émanant de locaux professionnels peuvent se trouver compris dans les notions de « vie privée » et de « correspondance » visés à l'article 8, paragraphe 1er de la CEDH[5]. Elle a par ailleurs estimé que les messages électroniques

3 Cour eur. D.H., 25 juin 1997, req. n° 20605/92, *Halford c. Royaume-Uni*, § 44 ; Cour eur. D.H., 3 avril 2007, req. n° 62617/00), *Copland c. Royaume-Uni*, § 41.

4 Cour eur. D.H., 3 avril 2007, req. n° 62617/00, *Copland c. Royaume-Uni*, § 41. Pour un commentaire de cet arrêt, voy. F. KÉFER et S. CORNELIS, « L'arrêt *Copland* ou l'espérance légitime du travailleur quant au caractère privé de ses communications. Cour européenne des droits de l'Homme (quatrième section), *Copland c. Royaume-Uni*, 3 avril 2007 », *Rev. Trim. D.H.*, 2009, vol. 79, pp. 779 et s.

5 Cour eur. D.H., 25 juin 1997, req. n° 20605/92, *Halford c. Royaume-Uni*, § 44 ; Cour eur. D.H., 3 avril 2007, req. n° 62617/00, *Copland c. Royaume-Uni*, § 41.

envoyés depuis le lieu de travail doivent jouir de la même protection au titre de l'article 8, tous comme les éléments recueillis au moyen de la surveillance de l'usage qu'une personne fait de Internet[6].

Dans ces décisions, la Cour tempère toutefois cette affirmation en précisant, dans chacune des affaires susmentionnées, que la travailleuse concernée n'ayant pas été prévenue de possibles mesures de contrôle sur son utilisation de cet outil, elle pouvait nourrir des attentes raisonnables en matière de vie privée[7-8]. Ce faisant, la Cour laisse entendre qu'il eut pu en être autrement si on avait informé l'intéressée de ce que l'utilisation du matériel était surveillée.

9. Le raisonnement est quelque peu différent dans la troisième affaire qu'a traitée la Cour et qui concernait la prise de connaissance et l'utilisation en justice de messages issus d'un compte de messagerie instantanée (*Yahoo Messenger*) créé par un travailleur à la demande de son employeur pour les besoins de sa fonction. Il s'agit de l'arrêt rendu par la Cour le 12 janvier 2016 dans l'affaire *Bărbulescu*[9]. Tout en invoquant la jurisprudence rappelée ci-avant, cette décision s'en démarque à plusieurs égards et a d'ailleurs été largement remise en cause dans l'arrêt intervenu le 5 septembre 2017[10] d'un renvoi devant la Grande chambre.

10. À l'origine du litige, un contrôle de cette messagerie sur laquelle il y avait eu quelques échanges privés avec des membres de la famille du travailleur et dont certains avaient trait à la vie sexuelle du travailleur. C'est l'utilisation des ressources informatiques à des fins privées en contravention des règles d'entreprise (et non la teneur des messages) qui avait conduit au licenciement du travailleur.

Dans son arrêt du 12 janvier 2016, la Cour laisse dans un premier temps entendre que ces messages sont susceptibles d'être protégés comme relevant de la vie privée et du droit à la correspondance mais

6 Cour eur. D.H., 3 avril 2007, req. n° 62617/00, *Copland c. Royaume-Uni*, § 41.

7 Cour eur. D.H., 25 juin 1997, req. n° 20605/92, *Halford c. Royaume-Uni*, § 44 ; Cour eur. D.H., 3 avril 2007, req. n° 62617/00), *Copland c. Royaume-Uni*, § 42.

8 On retrouvera ce critère également dans un arrêt *Peev* qui concerne la fouille d'un tiroir de bureau (Cour eur. D.H., 26 juillet 2007, req. n° 64209/01, *Peev c. Bulgarie*). Là encore, c'est ce critère d'attente raisonnable ou espérance légitime qui est mis en exergue par la Cour pour déterminer s'il y a ingérence ou non dans la vie privée. Les enseignements de cet arrêt nous paraissent pertinents également en ce qui concerne l'usage d'un ordinateur, par exemple, l'arrêt *Libert* (22 février 2018) évoqué *infra* aborde précisément cette situation. L'absence d'une information préalable d'une travailleuse concernant l'installation d'une caméra cachée de vidéosurveillance a également été considérée comme une ingérence dans la vie privée de cette dernière (Cour eur. D.H., 15 octobre 2010, req. n° 420/07, *Köpke c. Allemagne* [déc.]).

9 Cour eur. D.H., 12 janvier 2016, req. n° 61496/08, *Bărbulescu c. Roumanie*.

10 Cour eur. D.H. (Gde ch.), 7 septembre 2017, req. n° 61496/08, *Bărbulescu c. Roumanie*.

précise ensuite qu'il convient de vérifier si M. Bărbulescu pouvait raisonnablement croire au caractère privé des communications échangées via le compte *Yahoo Messenger* qu'il avait créé à la demande de son employeur[11]. Elle constate qu'un règlement intérieur interdisait tout usage privé des ressources et ordinateurs de l'employeur mais qu'il existait un doute qu'en au fait que M. Bărbulescu avait été informé d'une possible prise de connaissance des messages échangés lors d'un contrôle. Curieusement, ce n'est pas ce constat que reprend la Cour pour finalement conclure à l'existence d'une ingérence. Elle met en exergue le fait que la teneur des communications du travailleur sur *Yahoo Messenger* a été consultée par l'employeur et que la transcription de ces communications a été utilisée par la suite dans le cadre de la procédure menée devant les juridictions du travail, pour considérer que ces mesures concernaient la « vie privée » et la « correspondance » de l'intéressé au sens de l'article 8, paragraphe 1er.

Par ailleurs, pour justifier le fait que M. Bărbulescu aurait dû être informé des mesures de contrôle dont il pouvait faire l'objet en rapport avec l'utilisation de cette messagerie, la Cour se fonde sur la législation en matière de protection de données à caractère personnel. Elle relève la condition d'information préalable qui doit être rencontrée pour ce qui concerne les traitements de données. Il nous semble qu'il s'agit d'un mélange des genres peu heureux dans le contexte d'une analyse visant à déterminer s'il y a ingérence dans la vie privée. En effet, certes la législation sur la protection des données à caractère personnel a vocation à s'appliquer dans ce genre de cas de figure[12], et nous y reviendrons (voy. section III *infra*), mais cette législation ne vise pas à protéger la vie privée en tant que telle. Elle a pour objectif d'assurer, lorsqu'une personne traite des données relatives à une personne physique, un équilibre entre les droits et intérêts des parties mais cette protection n'est pas conditionnée au fait que la donnée relève de la vie privée de la personne concernée. Or, ce que la Cour tentait d'établir était précisément de déterminer si on pouvait parler d'ingérence dans la vie privée du travailleur.

11. Plus fondamentalement, on peut s'interroger sur le fait de savoir si cela a un sens d'assimiler attentes raisonnables et information préalable. Si un employeur décide de mesures particulièrement invasives, comme par exemple d'enregistrer toutes les conversations téléphoniques de tous ses employés et les en informe, cela impliquerait-il qu'il y ait

11 Cour eur. D.H., 12 janvier 2016, req. n° 61496/08, *Bărbulescu c. Roumanie*, §§ 36 et s.
12 *Ibid.*, § 42.

attentes raisonnables et donc inexistence d'une ingérence ? À notre sens, il conviendrait de détacher les deux concepts et d'envisager si l'existence d'un espace vital d'« intimité » n'est pas à ménager en toute hypothèse[13]. Rien n'empêche dans un second temps de considérer que l'acte d'ingérence qui aurait pris la forme d'une mesure de contrôle par exemple, est admissible au regard des critères de légalité, finalité, et proportionnalité.

12. L'arrêt rendu par la Grande chambre le 5 septembre 2017 dans la même affaire *Bărbulescu* va résolument dans ce sens. La Cour explicite davantage ce que recouvre la notion de vie privée et de correspondance dans un contexte professionnel. Elle précise notamment que « des restrictions apportées à la vie professionnelle peuvent tomber sous le coup de l'article 8 lorsqu'elles se répercutent sur la façon dont l'individu forge son identité sociale par le développement de relations avec autrui »[14]. Quant à la notion de « correspondance », la Cour souligne le fait qu'aucun adjectif n'accompagne ce terme de sorte que le fait que la correspondance soit échangée dans un contexte professionnel n'empêche pas l'application de l'article 8 de la CEDH[15]. La Cour rappelle ensuite le critère important mais non décisif, pour que l'on puisse conclure à l'applicabilité des notions de vie privée et de correspondance, à savoir celui des attentes raisonnables de l'individu quant à une protection et au respect de celles-ci.

Ce qui est remarquable dans le raisonnement de la Cour par rapport à l'affaire tranchée, c'est qu'elle va constater que le travailleur avait été informé de l'interdiction de tout usage privé des ressources informatiques et de possibles contrôles (seul restant incertain, le degré de précision dans l'étendue et de la portée de la surveillance), mais va conclure à une ingérence dans la vie privée et la correspondance de M. Bărbulescu. En effet, la Cour concède qu'« il n'est pas certain que les règles restrictives de l'employeur aient laissé au requérant une attente raisonnable en matière de vie privée – attente dont la mesure resterait à déterminer » avant de considérer que « les instructions d'un employeur ne peuvent

13 En ce sens, le Groupe de l'Article 29 rappelle, dans un document de travail consacré à la problématique de la surveillance des communications électroniques sur le lieu du travail, qu'un travailleur peut légitimement s'attendre au respect de sa vie privée même lorsqu'il utilise des outils de communications professionnels. Il considère que la fourniture d'informations adéquates au travailleur concernant les règles d'utilisation des outils de communication et les mesures de contrôles mises en place peut *diminuer* ses attentes raisonnables en termes de respect de la vie privée (Groupe de l'Article 29, document de travail concernant la surveillance des communications électroniques sur le lieu du travail, 29 mai 2002, WP 55, p. 9). Voy. également à ce sujet la section III.

14 Cour eur. D.H. (Gde ch.), 7 septembre 2017, req. n° 61496/08, *Bărbulescu c. Roumanie*, § 70.

15 *Ibid.*, § 71.

pas réduire à néant l'exercice de la vie privée sociale sur le lieu de travail. Le respect de la vie privée et de la confidentialité des communications continue à s'imposer, même si ces dernières peuvent être limitées dans la mesure du nécessaire »[16].

Autrement dit, des instructions visant à réduire tout espace de communications à des fins autres que strictement professionnelles ne donnent pas à l'employeur un blanc-seing pour exercer une surveillance sur l'usage de ces outils de communications.

On retiendra de ce qui précède que les communications échangées à partir du lieu du travail bénéficient de la protection de l'article 8 et que l'un des critères mobilisés pour vérifier l'existence d'une ingérence est lié aux anticipations que le travailleur pouvait nourrir concernant le contrôle, voire la prise de connaissance, de ses communications. L'absence de règles communiquées au travailleur peut conduire à la constatation de l'absence d'attentes raisonnables dans son chef mais l'existence de règles trop intrusives peuvent également amener au même constat.

B. – *Les conditions d'admissibilité de l'ingérence*

Les trois conditions d'admissibilité qui sont dégagées du texte de l'article 8, paragraphe 2 de la CEDH, sont les principes de légalité, de finalité et de proportionnalité.

1. – *Critère de légalité*

13. La jurisprudence de la Cour européenne des droits de l'homme consacrée spécifiquement à la question du contrôle de l'usage des outils de communication sur le lieu du travail est plutôt maigre à cet égard.

En effet, dans deux premiers arrêts phares qui ont été rendus dans ce domaine, à savoir les arrêts précités *Halford* et *Copland*, la Cour a constaté que c'était le principe de légalité qui n'avait pas été rencontré. Il s'agissait de cas dans lesquels l'employeur était un établissement dirigé par l'État. La Cour a donc analysé la question en se penchant sur les dispositions légales qui existaient en la matière et leur caractère suffisamment spécifique ou non et, à chaque fois, elle a constaté qu'il n'existait pas de règles de loi suffisamment précises et prévisibles.

16 *Ibid.*, § 79.

Dans ses arrêts, la Cour rappelle que par les termes « prévue par la loi », on entend une règle de droit interne qui doit offrir une certaine protection contre les atteintes arbitraires de la puissance publique aux droits garantis par le paragraphe premier de l'article 8 et que la qualité de la loi doit être conforme aux principes caractérisant l'État de droit. Cette loi doit rencontrer une exigence de prévisibilité et user de termes assez clairs pour indiquer à tous de manière suffisante en quelles circonstances et sous quelles conditions elle habilite la puissance publique à prendre pareille mesure[17].

14. Ce cas de figure ne correspond pas à la plupart des hypothèses où c'est un employeur du secteur privé qui procède à une mesure de contrôle problématique.

On notera qu'il y a dans ce cas de figure une application horizontale de la Convention européenne des droits de l'homme, en ce sens que les droits et libertés qu'elle reconnaît sont invoqués dans un litige entre particuliers, et non entre un État et un individu[18].

L'impact de cet effet horizontal se traduit par une approche un peu différente de la Cour quant à l'analyse d'une possible violation de l'article 8. La violation est toujours imputée à un État, non en raison d'une ingérence dans son chef, mais plutôt en raison d'un manquement à assurer le respect de ce droit dans les relations interindividuelles. Dans l'arrêt *Bărbulescu* du 12 janvier 2016, la Cour rappelle que, « si l'article 8 tend pour l'essentiel à prémunir l'individu contre des ingérences arbitraires des pouvoirs publics, il ne commande pas seulement à l'État de s'abstenir de pareilles ingérences : à cet engagement négatif peuvent s'ajouter des obligations positives inhérentes à un respect effectif de la vie privée. Ces obligations peuvent impliquer l'adoption de mesures visant au respect de la vie privée jusque dans les relations des individus entre eux (*Von Hannover c. Allemagne (n° 2)* [GC], nos 40660/08 et 60641/08, § 98, CEDH 2012, et *Benediksdóttir c. Islande* (déc.), n° 38079/06, 16 juin 2009). La frontière entre les obligations positives et négatives de l'État au titre de l'article 8 ne se prête pas à une définition précise. Dans les deux cas, il faut avoir égard au juste équilibre à ménager entre les intérêts concurrents – qui peuvent comprendre des intérêts privés et des intérêts publics concurrents ou différents droits protégés

17 Cour eur. D.H., 25 juin 1997, req. n° 20605/92, *Halford c. Royaume-Uni*, § 49 ; Cour eur. D.H., 3 avril 2007, req. n° 62617/00), *Copland c. Royaume-Uni*, §§ 45 et 46 ; Cour eur. D.H., 22 février 2018, req. n° 588/13, *Libert c. France*, §§ 43 et 44.

18 Voy. F. SUDRE, *Droit européen et international des droits de l'homme*, 6e éd., Paris, PUF, 2003, pp. 234 et s.

par la Convention (*Evans c. Royaume-Uni* [GC], n° 6339/05, §§ 75 et 77, CEDH 2007 I) – de même, dans les deux hypothèses, l'État jouit d'une certaine marge d'appréciation (*Von Hannover*, précité, et *Jeunesse c. Pays-Bas* [GC], n° 12738/10, § 106, 3 octobre 2014) »[19].

Ce qui est troublant dans l'arrêt *Bărbulescu* du 12 janvier 2016, c'est que la Cour ne vérifie pas l'existence d'une règle – fût-ce interne – qui prévoyait spécifiquement la possibilité et les modalités de ce contrôle. Elle raisonne uniquement dans le contexte de l'exercice du pouvoir disciplinaire que conférait à l'employeur le Code du travail roumain. Le Code du travail en vigueur au moment des faits disposait que l'employeur avait le droit de contrôler la manière dont les employés accomplissaient leurs tâches professionnelles. Cette disposition ne nous paraît pas des plus prévisibles tant elle est vaste. Et si l'on veut bien admettre, comme le fait la Cour par ailleurs, qu'il ne va pas de soi qu'un employeur contrôle la messagerie électronique de ses travailleurs, on ne s'explique pas que la Cour se satisfasse d'une norme aussi générale.

Cela a d'ailleurs donné lieu à une opinion partiellement dissidente dans le chef du Juge Pinto de Albuquerque qui a fait valoir que l'employeur qui veut opérer des contrôles sur l'usage de la messagerie électronique ou d'Internet doit non seulement définir des règles d'utilisation mais également fournir une information suffisamment précise quant aux contrôles dont un travailleur peut faire l'objet[20].

Dans le prolongement des difficultés liées à l'application horizontale de l'article 8, certains auteurs relèvent dans le même sens que le critère de légalité devrait se traduire par une prise en compte des règles internes de l'entreprise[21]. Cela rejoindrait ainsi l'exigence de transparence qui reçoit une consécration spécifique sous l'angle de du droit à la protection des données[22].

15. L'analyse que livre la Grande chambre dans l'affaire *Bărbulescu* quant au respect de l'article 8 prend résolument une autre perspective liée à l'application horizontale de la Convention. En effet, elle dégage des critères à vérifier par la juridiction nationale saisie sans véritablement consacrer l'obligation pour l'État de prévoir une règlementation

19 Cour eur. D.H., 12 janvier 2016, req. n° 61496/08, *Bărbulescu c. Roumanie*, § 52.

20 Opinion partiellement dissidente du Juge Pinto de Albuquerque à la suite de l'arrêt *Bărbulescu c. Roumanie*, 12 janvier 2016, req. n° 61496/08, §§ 9 et s.

21 J.-P. MARGUÉNAUD et J. MOULY, « Big Boss is watching you – Alerte sur le contrôle des activités électroniques du salarié. Obs. sous Cour eur. D.H., arrêt *Bărbulescu c. Roumanie*, 12 janvier 2016 », *Rev. trim. D.H.*, 2016, vol. 108, p. 1045.

22 Voy. section III, *infra*.

spécifique. La raison de cette approche repose sur le constat selon lequel le droit du travail laisse une large part d'autonomie contractuelle et qu'il n'y a pas de consensus observé au niveau des États européens sur des règles arbitrant entre les droits et intérêts des parties concernées. La Cour constate en effet que peu d'États ont encadré de manière spécifique cette question de la surveillance des communications électroniques[23].

Elle reporte alors son contrôle, non sur la manière dont l'État a assuré au travers du cadre normatif une protection de l'individu[24], mais sur la manière dont les juridictions saisies du litige ont pris en compte dans leur analyse des critères que la Cour dégage par ailleurs et qui permettent de vérifier si un juste équilibre entre les intérêts en jeu a été ménagé[25]. Nous reviendrons sur ces critères dans les sections suivantes mais ils peuvent être résumés comme suit, selon des termes largement empruntés à la Cour :

– Le fait que l'employé ait été ou non informé (i) de la possibilité que l'employeur prenne des mesures de surveillance de sa correspondance et de ses autres communications, (ii) de la nature de cette surveillance, ainsi que (iii) de la mise en place de telles mesures avant que celle-ci n'intervienne ;
– Le fait que l'étendue de la surveillance opérée par l'employeur et le degré d'intrusion dans la vie privée de l'employé (par exemple, accès ou non au contenu des communications) soient ou non justifiés par des motifs légitimes avancés par l'employeur ;
– Le fait que la mise en place d'un système de surveillance reposant sur des moyens et des mesures moins intrusives ou n'impliquant pas un accès direct au contenu des communications de l'employé, le cas échéant, aurait pu être envisagée au regard des motifs de la surveillance ;
– Le fait que les résultats de la surveillance ont été ou non effectivement utilisés pour atteindre le but fixé ;

23 Cour eur. D.H. (Gde ch.), 7 septembre 2017, req. n° 61496/08, *Bărbulescu c. Roumanie*, §§ 117 et s.

24 Il est juste fait référence au fait que les autorités internes doivent veiller à ce que les employés dont les communications ont été surveillées puissent bénéficier d'une voie de recours devant un organe juridictionnel ayant compétence pour statuer, du moins en substance, sur le respect des critères énoncés par la Cour ainsi que sur la licéité des mesures contestée (Cour eur. D.H. (Gde ch.), 7 septembre 2017, req. n° 61496/08, *Bărbulescu c. Roumanie*, § 122).

25 Cour eur. D.H. (Gde ch.), 7 septembre 2017, req. n° 61496/08, *Bărbulescu c. Roumanie*, §§ 124 et s. Plusieurs juges entendent toutefois se démarquer de cet aspect de la décision dans une opinion dissidente. Ils estiment que le cœur des obligations positives de l'État se situe dans la mise en place d'un cadre normatif et de recours internes et qu'il n'y avait pas lieu de se focaliser sur le travail d'analyse des juridictions du travail, sans égard au fait qu'il existait d'autres possibilités de recours en droit roumain non mises en œuvre par le requérant et qui lui permettaient de faire valoir une protection contre les ingérences dénoncées (opinion dissidente des Juges RAIMONDI, DEDOV, KJØLBRO, MITS, MOUROU-VIKSTRÖL et EICKE).

– Les conséquences de la surveillance pour l'employé qui en a fait l'objet, notamment en termes de proportionnalité de la sanction prise à la suite de la surveillance ;
– La mise en place ou non de garanties adéquates, notamment lorsque les mesures de surveillance de l'employeur avaient un caractère intrusif. Et la Cour de préciser que « [c]es garanties doivent notamment permettre d'empêcher que l'employeur n'ait accès au contenu même des communications en cause sans que l'employé n'ait été préalablement averti d'une telle éventualité »[26].

16. À ce stade, nous nous arrêterons à l'examen de l'exigence de transparence induite du premier critère dégagé par la Cour. Celle-ci implique que les juridictions nationales saisies vérifient si le travailleur a été averti des mesures de surveillance, mais pas uniquement. L'information doit également porter sur l'étendue de la surveillance et sur le fait que l'employeur accèdera ou non au contenu des communications[27]. Cette information doit en outre être préalable à la mise en place de la surveillance.

La Cour souligne par ailleurs que, lorsqu'un accès au contenu des communications est envisagé, le moment où cet accès est réalisé et la transparence de l'employeur à cet égard doivent également être pris en compte dans l'analyse de la balance des intérêts des parties[28]. Ces exigences sont sans doute inspirées par la circonstance que, dans l'affaire impliquant M. Bărbulescu, ce dernier faisait grief à son employeur d'avoir procédé à la surveillance, opéré une transcription du contenu de ses communications et de les avoir consultées avant de l'interpeller et de lui avoir demandé s'il avait ou non utilisé la messagerie à des fins privées sans l'informer des données dont l'employeur disposait déjà. L'employeur n'avait présenté, lors de cette première interpellation, que des graphiques comparant le trafic internet de M. Bărbulescu par rapport à ses collègues. Ce n'est que lorsque M. Bărbulescu a répondu qu'il n'avait fait qu'un usage professionnel du compte *Yahoo Messenger* qu'on lui a communiqué, cinquante minutes plus tard, la copie des transcriptions du contenu des communications[29].

26 Cour eur. D.H. (Gde ch.), 7 septembre 2017, req. n° 61496/08, *Bărbulescu c. Roumanie*, § 121.
27 *Ibid.*, § 133.
28 *Ibid.*, § 138.
29 *Ibid.*, § 130.

2. – *Critère de finalité*

17. Ce phénomène d'horizontalisation de l'application de la CEDH pose de nouvelles questions et de nouveaux défis puisqu'en ce qui concerne le second critère de l'article 8, paragraphe 2, CEDH, à savoir celui des finalités, il implique de transposer les finalités reprises dans cette disposition, et pensées au départ pour encadrer des ingérences de l'autorité publique dans la vie privée des citoyens, à une situation où il s'agit de deux particuliers ou deux individus ou d'une société et un individu qui sont concernés.

On voit, à travers la jurisprudence de la Cour européenne des droits de l'homme, que de nouvelles finalités se dessinent concernant les éléments à prendre en compte dans la balance pour vérifier s'il s'agit d'une finalité légitime et proportionnée.

Dans l'arrêt du 12 janvier 2016 rendu dans l'affaire *Bărbulescu*, la Cour met en exergue « qu'il n'est pas déraisonnable pour un employeur de vouloir vérifier que ses employés accomplissent leurs tâches professionnelles pendant leurs heures de travail »[30]. Ceci est d'ailleurs confirmé par la Grande chambre dans son arrêt précité du 5 septembre 2017 qui évoque plus largement un intérêt légitime à assurer le bon fonctionnement de l'entreprise, ce qui peut se traduire par la mise en place des mécanismes lui permettant de vérifier que ses employés accomplissent leurs tâches professionnelles « de manière adéquate et avec la célérité requise »[31].

Cette finalité nous semble pouvoir être rattachée à un intérêt plus large de l'employeur à préserver ses intérêts économiques comme illustré dans un arrêt *Köpke c. Allemagne* du 5 octobre 2010. Dans cet arrêt, la Cour européenne des droits de l'homme se penche plus spécifiquement sur la question *du droit à se constituer une preuve*, et ce dans un contexte qui est celui de la surveillance sur le lieu du travail[32]. Il est rendu dans une affaire de vidéosurveillance cachée, mise en place par un détective privé à la demande d'un employeur pour identifier le responsable de détournement d'une partie des recettes à la caisse d'un supermarché[33]. L'employeur avait licencié la travailleuse qui avait pu être identifiée de cette manière comme étant l'auteur de ces irrégularités.

30 Cour eur. D.H., 12 janvier 2016, req. n° 61496/08, *Bărbulescu c. Roumanie*, §§ 59 et 127.
31 Cour eur. D.H. (Gde ch.), 7 septembre 2017, req. n° 61496/08, *Bărbulescu c. Roumanie*, § 127 ; Cour eur. D.H., 22 février 2018, req. n° 588/13, *Libert c. France*, § 46.
32 Cour eur. D.H., 5 octobre 2010, req. n° 420/07, *Köpke c. Allemagne* (déc.).
33 *Ibid*.

La travailleuse invoquait la violation de l'article 8 CEDH qui résidait tant dans la mise en place de la vidéosurveillance sur le lieu du travail sans qu'elle en ait été informée, que dans la production des preuves ainsi recueillies en justice. La Cour, constatant que les images ainsi obtenues avaient été traitées et examinées par plusieurs personnes travaillant pour l'employeur et avaient été utilisées dans le cadre d'une procédure devant les juridictions du travail, conclut à une ingérence dans la vie privée de la travailleuse.

Dans le cadre de l'examen du caractère admissible ou non de l'ingérence, la Cour met en balance les intérêts respectifs du travailleur et de l'employeur. Elle constate que l'intérêt de l'employeur à la protection de ses droits de propriété ne peut être efficacement sauvegardé que s'il peut recueillir des preuves permettant de prouver le comportement fautif (et en l'occurrence infractionnel) de la travailleuse devant les juridictions du travail et conserver lesdites preuves jusqu'à ce qu'une décision judiciaire définitive intervienne. La Cour souligne également que cette possibilité peut servir un intérêt public, à avoir une bonne administration de la justice par les tribunaux nationaux en leur permettant d'être en mesure d'établir autant que possible la vérité, tout en respectant les droits de la Convention de l'ensemble des personnes concernées. La Cour pointe en outre qu'en l'espèce la surveillance secrète aura permis de laver de tout soupçon les autres employés du magasin.

3. – *Critère de proportionnalité*

18. Principe de proportionnalité appliqué à la finalité poursuivie. La doctrine soutient que la dimension « horizontale » de la CEDH doit mener la Cour de Strasbourg à repenser son test de proportionnalité lorsqu'est en cause une relation interindividuelle (et notamment une relation de travail) dans le sens d'une « proportionnalité privatisée », c'est-à-dire d'une mise en balance d'intérêts exclusivement privés, dans la mesure où la « proportionnalité publique » ne serait pas totalement transposable aux relations privées[34].

Ce type de contrôle de proportionnalité privatisée peut être identifié dans une décision du 28 juin 2001, dans laquelle la Cour européenne des droits de l'homme a conclu à l'absence de tout manquement de la

[34] V. VAN DER PLANCKE et N. VAN LEUVEN, « La privatisation du respect de la Convention européenne des droits de l'homme : faut-il reconnaître un effet horizontal généralisé ? », *CRIDHO Working Paper*, 2007, n° 54, http://cridho.cpdr.ucl.ac.be/documents/Working.Papers/CRIDHO.WP2007-3.pdf.

Suisse à son obligation de protéger le droit au respect de la vie privée d'un individu qui avait fait l'objet, à son insu, d'investigations par un assureur : « [l]a Cour note que les juges nationaux ont fait une analyse approfondie des intérêts concurrents existant entre l'assureur et la requérante. […] Ils ont retenu qu'en l'espèce, les investigations de l'assureur, effectuées à partir du domaine public et limitées à la constatation de la mobilité de la requérante, visaient uniquement à préserver les droits patrimoniaux de l'assurance. Les juges ont ainsi reconnu un intérêt prépondérant à l'assureur et en ont conclu que l'atteinte à la personnalité de la requérante n'était pas illicite »[35].

Cette mise en balance est également particulièrement mise en exergue dans le cadre de l'arrêt *Bărbulescu* du 12 janvier 2016 qui énonce que « [l]a Cour doit donc déterminer si, dans le cadre des obligations positives que lui impose l'article 8, l'État a ménagé un juste équilibre entre le droit du requérant au respect de sa vie privée et de sa correspondance et les intérêts de l'employeur de l'intéressé »[36]. Nous avons signalé que cette position avait été quelque peu revue dans l'arrêt de la Grande chambre rendu dans la même affaire le 5 septembre 2017. Nous nous proposons d'évoquer le premier arrêt pour mettre en évidence en quoi celui rendu par la Grande chambre s'en démarque.

Dans l'arrêt du 12 janvier 2016, la Cour relève que l'intérêt de l'employeur pris en compte était celui de vérifier que les employés accomplissent leurs tâches professionnelles pendant leurs heures de travail, et ce alors même que l'employeur ne faisait état d'aucun préjudice spécifique. La Cour ne donne toutefois que peu d'indications sur le poids à donner à cet intérêt. En effet, dans son arrêt la Cour prend soin d'indiquer qu'en l'occurrence l'employeur avait agi sur la foi des déclarations du travailleur, en pensant que le compte de messagerie qu'elle allait contrôler ne contenait que des messages à caractère professionnel. On peut penser à un contrôle ayant pour but de vérifier que le travailleur répondait effectivement aux questions qui lui étaient posées par des clients de l'entreprise comme il était censé le faire. Ceci étant, la Cour ne semble pas consacrer un droit absolu de l'employeur d'accéder à une boîte de messagerie mais uniquement le subordonner à une mise en balance dont il est difficile de dégager des lignes fortes. Qu'en eût-il été si l'employeur n'avait pas reçu l'assurance que le compte de contenait que des messages professionnels ? La question est d'autant

35 Cour eur. D.H., 28 juin 2001, req. n° 41953/98, *Verlière c. Suisse* (déc.).
36 Cour eur. D.H., 12 janvier 2016, req. n° 61496/08, *Bărbulescu c. Roumanie*, § 54.

plus pertinente qu'en règle c'est souvent l'usage « privé » d'un outil de communication qui amène à poser le problème du droit au respect de la vie privée.

La Grande chambre estime, quant à elle, que l'examen réalisé par les juridictions nationales est trop léger et qu'il n'a pas été vérifié quelles étaient concrètement les raisons légitimes qui avaient poussé en l'occurrence l'employeur à enregistrer en temps réel toutes les communications (connexions à la messagerie instantanée) passées par le travailleur pendant une période de plusieurs jours. L'employeur avait, à la suite de cette surveillance, présenté une transcription de quarante-cinq pages de communications échangées sur les deux comptes de messageries du travailleur. L'employeur n'avait pourtant évoqué aucun risque particulier qui aurait nécessité qu'une telle surveillance soit mise en place[37].

L'analyse des droits et intérêts des parties n'est pas en soi toujours concluante et est de fait complétée par des considérations qui concernent davantage la question du caractère proportionné des actes qui sont posés.

19. Principe de proportionnalité appliqué à l'acte d'ingérence. Quant aux exigences en termes de proportionnalité de la mesure par rapport au but recherché, il est affaire d'appréciation au cas par cas.

Par exemple, dans l'arrêt *Köpke c. Allemagne* du 5 octobre 2010 précité, la Cour a examiné le caractère proportionné de l'ingérence et relevé que les juridictions nationales avaient constaté qu'il n'y avait pas d'autre moyen de se ménager une preuve qui aurait pu offrir la même efficacité en créant une ingérence moindre dans le droit de la travailleuse au respect de sa vie privée[38].

20. Dans le premier examen de l'affaire *Bărbulescu* en 2016, la Cour prend différents éléments en considération, à commencer par le fait que le contenu des communications électroniques avait été retranscrit à titre de preuve mais non exploité pour justifier la sanction disciplinaire qui avait donné suite au contrôle[39]. En effet, ce qui avait été reproché c'était d'avoir utilisé la messagerie à des fins privées mais non le contenu des messages. Ont été également pris en compte le fait que le contrôle avait été limité au compte de messagerie (les fichiers stockés sur le disque dur de l'ordinateur n'avaient fait l'objet d'un contrôle) et le fait que le

37 Cour eur. D.H. (Gde ch.), 7 septembre 2017, req. n° 61496/08, *Bărbulescu c. Roumanie*, § 133.
38 Cour eur. D. H., 5 octobre 2010, req. n° 420/07, *Köpke c. Allemagne*.
39 Cour eur. D.H., 12 janvier 2016, req. n° 61496/08, *Bărbulescu c. Roumanie*, § 58.

travailleur n'avait pas fourni d'explications convaincantes sur le motif qui l'avait amené à utiliser le compte à des fins privées[40].

Par contre, il n'est dit mot de la façon dont le contrôle avait été opéré. Or, dans les débats qui ont été tenus lors de l'audience devant la Grande chambre[41], les conseils de M. Bărbulescu ont expliqué que le compte avait été « espionné » pendant plusieurs jours. Ils précisent que l'employeur disposait d'ailleurs du résultat de cette surveillance avant d'interpeller M. Bărbulescu pour qu'il confirme s'il avait ou non fait un usage non professionnel du compte. L'employeur plaidait quant à lui qu'il n'avait examiné les copies recueillies qu'après avoir reçu confirmation de ce que l'usage était strictement professionnel.

Il peut paraître étonnant que la Cour n'ait pas accordé d'attention à la manière dont le contrôle avait été mené techniquement, et ce pour deux raisons au moins. Tout d'abord, sur le plan des attentes raisonnables : lorsque l'employeur a recours à un logiciel particulièrement intrusif, à l'insu du travailleur, ce dernier peut-il véritablement concevoir qu'un tiers aura accès au contenu d'une boîte de messagerie, d'autant qu'en l'espèce le compte avait été créé au nom du travailleur par ce dernier auprès du fournisseur de services, l'employeur n'ayant jamais obtenu ni sollicité un quelconque moyen pour y accéder.

Par ailleurs, le caractère assez intrusif des moyens de contrôle sur le plan technique n'a pas été pris en considération comme élément d'appréciation. Dans la décision Köpke, la Cour avait laissé entendre qu'il s'agissait d'un élément de poids à prendre en compte dans la mise en balance. Elle avait en effet ponctué son raisonnement de la conclusion suivante : « [t]he competing interests concerned might well be given a different weight in the future, having regard to the extent to which intrusions into private life are made possible by new, more and more sophisticated technologies »[42].

L'arrêt de la Grande chambre dans l'affaire *Bărbulescu* redresse la barre. Il souligne le caractère particulièrement intrusif de la surveillance quant à l'ampleur du contrôle sur plusieurs jours et moyennant un enregistrement systématique, incluant en outre le contenu des communications, ainsi que l'absence d'une attention suffisante portée au caractère

40 *Ibid.*, §§ 60 et 61.

41 L'enregistrement de l'audience est disponible sur http://www.echr.coe.int.

42 Traduction libre : « [l]es intérêts concurrents concernés pourraient à l'avenir se voir donner un poids différent, en ayant égard à l'étendue des intrusions dans la vie privée qui deviennent possibles par le biais de technologies nouvelles et de plus en plus sophistiquées » (Cour eur. D. H., 5 octobre 2010, req. n° 420/07, *Köpke c. Allemagne*).

proportionné et nécessaire de ces mesures par rapport à une finalité légitime dont aurait pu se prévaloir l'employeur[43].

21. Les solutions contradictoires dégagées par la Cour dans les deux arrêts *Bărbulescu* sont le résultat d'une appréciation par rapport aux éléments spécifiques de la cause. Ces éléments sont illustratifs de la difficulté qui existe de longue date d'arbitrer entre les droits du travailleur et les intérêts de l'employeur lorsqu'il est question de l'usage de technologies qui ont profondément modifié les modes et habitudes de communication, avec les risques d'abus d'utilisation qu'elles rendent possibles, que ce soit dans le chef du travailleur ou de l'employeur. On en trouve encore une illustration au travers de l'arrêt *Libert* qui concernait la prise de connaissance de fichiers sur un support de l'employeur[44]. Dans cette affaire, la Cour vérifie si l'ingérence consistant en une prise de connaissance de fichiers sur le disque dur d'un travailleur par un employeur assimilé à une autorité publique (en l'occurrence, la SNCF), est admissible. Sur la question de la proportionnalité, la Cour va estimer que les juridictions nationales ont pu considérer que l'accès aux fichiers par l'employeur pouvait dans ce cas intervenir hors de la présence du travailleur en application d'un règlement interne qui ne prévoyait de mesures spécifiques que lorsqu'il s'agissait d'accéder à des documents privés. La particularité du cas est que les fichiers étaient sauvegardés sur un espace disque habituellement réservé aux fichiers professionnels et que la dénomination du dossier ne correspondait pas à celle prévue dans ce règlement pour identifier les fichiers personnels. La différence était mince puisque le travailleur avait nommé le dossier « dossiers personnels » alors que le règlement imposait qu'il soit fait référence à un caractère « privé » du dossier. On peut donc avoir l'impression que la Cour lâche un peu du lest concernant le respect de la vie privée du travailleur, en cautionnant en quelque sorte une application extrêmement stricte du règlement interne de l'entreprise. Une autre lecture est, selon nous, possible : la Cour souligne en effet toute une série de considérations factuelles qui pouvaient justifier qu'en l'espèce les juridictions nationales s'emploient à une application rigoureuse, voire tatillonne du règlement, et principalement le caractère particulièrement volumineux du dossier qui comptait pas moins de 1582 fichiers tandis que la dénomination

[43] Cour eur. D.H. (Gde ch.), 7 septembre 2017, req. n° 61496/08, *Bărbulescu c. Roumanie*, §§ 135 et 136.
[44] Cour eur. D.H., 22 février 2018, req. n° 588/13, *Libert c. France*.

« documents personnels » pouvait tout aussi bien faire référence à des dossiers gérés personnellement par le travailleur.

22. Principe de proportionnalité appliqué à la sanction. La question la proportionnalité de la mesure adoptée par l'employeur sous l'angle de la sanction a été abordée par le Juge Pinto de Albuquerque dans une opinion partiellement dissidente émise à la suite de l'arrêt *Bărbulescu* de 2016. Un licenciement est en effet une mesure lourde de conséquences pour le travailleur. Or dans l'affaire *Bărbulescu*, il n'était invoqué à l'appui du licenciement qu'un manquement aux règles internes de l'entreprise (interdiction absolue de l'usage à des fins privées des outils de communication) sans qu'on ait égard à l'existence d'un réel préjudice dans le chef de l'entreprise ni d'un comportement problématique dans la durée dans le chef du travailleur. Comme le font remarquer J.-P. Marguénaud et J. Mouly, la Cour, en faisant l'économie de cette analyse, semblait consacrer le droit pour l'employeur de s'assurer « par les moyens les plus disproportionnés qu'il n'y aurait pas, qu'il n'y aurait plus, la moindre entorse à l'exclusivité de l'activité professionnelle pendant [l]es heures de travail »[45]. Il n'y avait pas de prise en compte de la gravité de mesure prise à l'encontre du travail comme faisant partie intégrante de l'analyse de proportionnalité.

L'arrêt de la Grande chambre, sur ce point encore, se distingue de la première décision rendue en épinglant l'absence de prise en compte de la proportionnalité de la mesure de licenciement[46].

C. – *Les liens avec un droit à l'usage d'Internet et la liberté d'expression*

23. En parallèle avec le droit à voir une certaine intimité préservée, même sur le lieu du travail, on peut s'interroger sur l'existence d'une obligation positive d'un employeur de permettre l'usage à des fins non strictement professionnelles d'outils de communications mis à disposition du travailleur. En effet, si la Cour constate, comme rappelé dans l'introduction, que c'est dans leur travail que la majorité des individus cultivent des liens sociaux, cela n'impliquerait-il pas un droit minimum à pouvoir communiquer dans et hors de l'entreprise via ces moyens de communications électroniques ? Autrement dit, le pouvoir de

45 J.-P. MARGUÉNAUD et J. MOULY, « Big Boss is watching you – Alerte sur le contrôle des activités électroniques du salarié. Obs. sous Cour eur. D.H., arrêt *Bărbulescu c. Roumanie*, 12 janvier 2016 », *op. cit.*, p. 1047.

46 Cour eur. D.H. (Gde ch.), 7 septembre 2017, req. n° 61496/08, *Bărbulescu c. Roumanie*, § 137.

l'employeur de définir des règles d'utilisation ne serait pas absolu mais devrait ménager un « espace vital » de communication sous couvert du droit au respect de la vie privée, voire du droit à la liberté d'expression.

Dans la l'arrêt *Bărbulescu* du 12 janvier 2016, la Cour rappelle que la notion de vie privée est une notion large qui englobe le droit pour l'individu de nouer et développer des relations avec ses semblables. Elle précise d'emblée qu'« [u]ne lecture large de l'article 8 ne signifie toutefois pas qu'il protège toute activité qu'une personne pourrait souhaiter pratiquer avec d'autres pour nouer et développer des relations : il ne protège pas, par exemple, des relations interpersonnelles d'un contenu si ample et indéterminé qu'aucun lien direct entre l'action ou l'inaction de l'État et la vie privée de l'intéressé n'est envisageable (voir, *mutatis mutandis*, *Botta c. Italie*, 24 février 1998, § 35, *Recueil des arrêts et décisions* 1998-I) »[47].

Autrement dit, il faut, pour que l'article 8 trouve à s'appliquer, qu'un lien puisse être établi avec la vie privée d'un individu. Le fait qu'il s'agisse de communications réalisées sur le lieu du travail ne l'exclut pas mais la Cour n'affirme pas l'existence d'un droit à l'usage de ces moyens de communication, ni de manière positive (consécration d'un droit pour le travailleur), ni de manière négative (interdiction d'un contrôle généralisé par l'employeur). Comme le relèvent J.-P. Marguénaud et J. Mouly, la Cour qui avait initié une jurisprudence dans les arrêts *Copland* et *Halford* tendant vers une consécration d'une « bulle privée » au travailleur n'a pas poursuivi en ce sens dans ce premier arrêt *Bărbulescu* du 12 janvier 2016. Elle laisse entendre qu'un employeur peut interdire tout usage des outils de communications sur le lieu du travail[48].

24. Dans son opinion partiellement dissidente, le juge Pinto de Albuquerque identifie en revanche des principes qui plaident en faveur d'une protection minimale. Il évoque l'existence de l'accès à Internet en tant que droit de l'homme soulignant que « [l]es États ne peuvent assurer la liberté individuelle de rechercher et de recevoir des informations et de s'exprimer s'ils ne respectent pas et ne promeuvent pas également le droit individuel au respect de la vie privée »[49]. Il défend également l'idée selon laquelle les droits de l'employeur ne justifient pas

47 Cour eur. D.H., 12 janvier 2016, req. n° 61496/08, *Bărbulescu c. Roumanie*, § 35.

48 J.-P. MARGUÉNAUD et J. MOULY, « Big Boss is watching you – Alerte sur le contrôle des activités électroniques du salarié. Obs. sous Cour eur. D.H., arrêt *Bărbulescu c. Roumanie*, 12 janvier 2016 », *op. cit.*, pp. 1041 et 1042.

49 Opinion partiellement dissidente du Juge Pinto de Albuquerque à la suite de l'arrêt *Bărbulescu c. Roumanie*, 12 janvier 2016, req. n° 61496/08, § 3.

un contrôle illimité des communications sur le lieu du travail et que ce contrôle doit faire l'objet d'une politique axée sur des finalités légitimes et des mesures proportionnées et adéquates au vu de celles-ci[50]. Un lien est également tissé avec la liberté d'expression au terme du constat suivant : « [à] notre époque où la technologie a estompé la frontière entre vie professionnelle et vie privée, et où certains employeurs autorisent les employés à utiliser le matériel de l'entreprise à des fins personnelles, tandis que d'autres leur permettent d'utiliser leur propre matériel à des fins professionnelles, et que d'autres encore laissent ces deux possibilités, le droit pour l'employeur de faire respecter certaines règles sur le lieu de travail et l'obligation pour l'employé de s'acquitter correctement de ses tâches professionnelles ne justifient pas un contrôle illimité de l'expression des employés sur Internet »[51]. De l'ensemble de l'argumentation développée, on comprend que cela englobe les communications via Internet, tel l'envoi de courriers électroniques ou d'une messagerie professionnelle.

25. Sans aller jusqu'à consacrer un droit à l'accès à des moyens de communications sur le lieu du travail, la Cour européenne des droits de l'homme rend un arrêt de principe important lorsqu'elle énonce, dans l'arrêt *Bărbulescu* du 5 septembre 2017, qu'un employeur ne peut, par le biais de l'exercice de l'autorité patronale, réduire à néant l'exercice d'une vie privée sociale sur le lieu du travail laquelle englobe les communications échangées à partir de ce lieu[52].

D. – *Conclusion*

26. Les principes qui gouvernent le droit au respect de la vie privée s'articulent donc autour de notions à apprécier selon la situation concrète.

Nous avons vu que l'évolution de la jurisprudence en matière d'ingérence dans la vie privée et la correspondance appliquée au contexte des contrôles de communications électroniques consacre une véritable protection du travailleur, nonobstant le contexte professionnel des communications ou de l'usage de ressources appartenant à l'employeur. Pour le reste, il s'agit d'appréciation au cas par cas dont aura vu qu'elle peut donner lieu à des arbitrages très différents, en témoignent les conclusions

50 *Ibid.*, § 13.
51 *Ibid.*, § 4.
52 Cour eur. D.H. (Gde ch.), 7 septembre 2017, req. n° 61496/08, *Bărbulescu c. Roumanie*, § 80.

opposées de la juridiction strasbourgeoise dans l'affaire *Bărbulescu*. Si dans le premier arrêt de 2016, la Cour concluait à l'absence de violation de l'article 8 de la CEDH, les critères d'analyse dégagés dans l'arrêt de 2017 l'amènent à la conclusion inverse.

La protection des données à caractère personnel ne contrarie pas ces critères et nous semble plutôt complémentaire. Elle offre en effet un cadre plus balisé et plus contraignant dès lors qu'elle détaille à la fois des conditions pour la mise en œuvre du traitement et des obligations spécifiques dans le chef des personnes qui le mettent en œuvre.

III. Le droit à la protection des données à caractère personnel[53]

A. – *Introduction*

27. Le droit à la protection des données à caractère personnel a été consacré, en tant que tel, à l'article 8 de la Charte des droits fondamentaux de l'Union européenne.

Dès avant cette consécration, plusieurs textes, émanant du Conseil de l'Europe[54] ou de l'Union européenne avait déjà dégagé des règles et principes pour protéger les données à caractère personnel.

Une réflexion avait été initiée il y a quelques années concernant l'opportunité d'adopter une directive spécifique au traitement de données à caractère personnel dans le contexte professionnel. C'est dans ce cadre que le Groupe de l'Article 29 a rendu un avis sur la question[55] et que la Commission avait lancé une procédure de consultation des partenaires sociaux[56]. Ces initiatives n'ont pas débouché sur un texte.

Le siège de la matière est donc le droit commun de celle-ci, à savoir jusqu'en 2018, la directive 95/46/CE du Parlement européen et du

53 Une partie de cette section reprend des passages actualisés de K. ROSIER, « La directive 2002/58/EC vie privée et communications électroniques et la directive 95/46/CE relative au traitement des données à caractère personnel : comment les (ré)concilier ? », in *Défis du droit à la protection à la vie privée*, Bruxelles, Academia Bruylant, 2008, pp. 327-354.

54 Voy. principalement la Convention 108 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel du 28 janvier 1981, qui a récemment fait l'objet d'une procédure de révision.

55 Groupe de l'Article 29, avis 8/2001 sur le traitement de données à caractère personnel dans le contexte professionnel, 13 septembre 2001, WP 48, p. 4.

56 La Commission a publié un document intitulé « Deuxième phase de consultation des partenaires sociaux sur la protection des données à caractère personnel des travailleurs », 2002, http://europa.eu/rapid/press-release_IP-02-1593_fr.htm.

Conseil du 24 octobre 1995 relative à la protection des personnes physique à l'égard du traitement de données à caractère personnel et à la circulation des données (la « directive 95/46/CE »)[57]. Nous évoquerons également, dans la section IV, la directive 2002/58/CE relative du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques[58].

La directive 95/46/CE est remplacée à dater du 25 mai 2018 par le Règlement général sur la protection des données[59] (« RGPD » ou le « Règlement »). L'option d'un règlement plutôt que d'une directive devrait *a priori* permettre une plus grande harmonisation des règles en la matière, en supprimant l'exercice de transposition dans les droits nationaux qui conduisait à des disparités d'un État à l'autre.

Cela étant, le RGPD laisse encore de nombreux champs d'intervention aux États membres et celui des relations de travail en fait partie.

L'article 88 du RGPD prévoit que :

> « 1. […] Les États membres peuvent prévoir, par la loi ou au moyen de conventions collectives, des règles plus spécifiques pour assurer la protection des droits et libertés en ce qui concerne le traitement des données à caractère personnel des employés dans le cadre des relations de travail, aux fins, notamment, du recrutement, de l'exécution du contrat de travail, y compris le respect des obligations fixées par la loi ou par des conventions collectives, de la gestion, de la planification et de l'organisation du travail, de l'égalité et de la diversité sur le lieu de travail, de la santé et de la sécurité au travail, de la protection des biens appartenant à l'employeur ou au client, aux fins de l'exercice et de la jouissance des droits et des avantages liés à l'emploi, individuellement ou collectivement, ainsi qu'aux fins de la résiliation de la relation de travail.
>
> 2. […] Ces règles comprennent des mesures appropriées et spécifiques pour protéger la dignité humaine, les intérêts légitimes et les droits fondamentaux des personnes concernées, en accordant une attention particulière à la transparence du traitement, au transfert de données à caractère personnel au sein d'un groupe d'entreprises, ou d'un groupe d'entreprises engagées dans une activité économique conjointe et aux systèmes de contrôle sur le lieu de travail.
>
> 3. […] Chaque État membre notifie à la Commission les dispositions légales qu'il adopte en vertu du paragraphe 1 au plus tard le 25 mai 2018 et, sans tarder, toute modification ultérieure les concernant ».

57 *J.O.C.E.*, L 281, 23 novembre 1995, pp. 0031-0050.
58 *J.O.C.E.*, L 20, 31 juillet 2002, pp. 0037-0047.
59 Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE.

Il ne s'agit donc pas d'un blanc-seing puisqu'il y est question de protection des personnes concernées. On ignore à l'heure où ces lignes sont rédigées ce qui fera l'objet de règlementations particulières. En droit belge, par exemple, il n'y avait pas de loi spécifique définissant des conditions de traitements de données dans le cadre des relations de travail. Des dispositions ont été adoptées dans des lois concernant diverses problématiques en renvoyant pour ce qui n'y était pas spécifiquement réglé à la loi générale transposant la directive 95/46/CE. Pour ce qui concerne le contrôle des *e-mails* et d'Internet, c'est une convention collective de travail qui a été adoptée en 2002 et elle n'a pas été modifiée depuis lors.

28. Il demeure que les principes déjà présents dans la directive 95/46/CE seront toujours applicables, raison pour laquelle l'analyse que nous proposerons s'y référera. Nous nous concentrerons dans le cadre de cette contribution sur les principes les plus essentiels issus de cette directive tels qu'ils ont été interprétés à ce jour. L'analyse n'est donc pas exhaustive, et n'aborde par exemple pas les restrictions aux traitements liés aux flux transfrontières. Eu égard à l'entrée en application du Règlement, il nous semble par ailleurs pertinent d'épingler certains aspects spécifiques de celui-ci, dont le renforcement des exigences en matière de consentement et le concept de « profilage » qui intègre la notion de « rendement au travail » dans sa définition.

B. – *La double casquette de l'employeur responsable du traitement*

29. Les dispositions de la directive 95/46/CE ont fait l'objet de nombreux commentaires. Il nous semble toutefois qu'on est loin d'avoir mesuré toutes les implications que la règlementation en matière de protection des données peut avoir. L'une d'elles concerne, nous semble-t-il, son application au courrier électronique. En effet, il est indéniable que la rédaction, l'enregistrement ou encore l'envoi d'un courrier électronique contenant des données à caractère personnel constitue bel et bien un traitement de données à caractère personnel. Il s'agit d'opérations effectuées à l'aide de procédés automatisés sur des données à caractère personnel. Cette conclusion est soutenue d'ailleurs par l'arrêt *Lindqvist* de la Cour de Justice de l'Union européenne au terme duquel la simple mention d'une donnée à caractère personnel sur un site internet emporte application de la directive[60]. Il n'est donc nul besoin d'un quelconque

[60] C.J.C.E., 6 novembre 2003, C-101/01, *Bodil Lindqvist*.

ordonnancement spécifique des données pour tomber sous le coup de l'application de la directive 95/46/CE. Ces enseignements ne sont pas remis en question par le Règlement.

Ceci nous amène à nous interroger sur l'identité du responsable des traitements relatifs à la correspondance par courrier électronique effectuée à partir de la boîte professionnelle du travailleur. Le « responsable du traitement est la personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement de données à caractère personnel »[61].

Dès lors que l'outil qu'est le courrier électronique est mis à la disposition des travailleurs par l'employeur et qu'il est utilisé dans le cadre des activités professionnelles du travailleur, on considérera sans difficulté que l'employeur est bien le responsable de ces traitements. En effet, dans ce cas, l'utilisation du courrier électronique interviendra dans le cadre d'un traitement, entendu comme un ensemble d'opérations appliquées à des données à caractère personnel, décidé par l'employeur (telles la gestion de la clientèle, la gestion des salaires, etc.). Dès lors que la correspondance par courrier électronique est envisagée comme une tâche accomplie par le travailleur dans le cadre de la mise en œuvre d'un traitement décidé par l'employeur, c'est ce dernier qui sera considéré comme responsable de traitement. Ces travailleurs n'auront pas même la qualité de sous-traitants dès lors qu'ils agissent sous son autorité.

Par contre, lorsqu'il s'agit d'un usage par le travailleur du courrier électronique à des fins autres que professionnelles (privées, politiques, liées à une seconde activité professionnelle…), il nous semble que c'est bien le travailleur qui aura la qualité de responsable de traitement puisqu'il traite des données à d'autres fins que celles mises en œuvre par l'employeur et qu'il a lui-même déterminées.

Il n'est pas toujours aisé de déterminer si un usage de courrier électronique se situe dans le cadre des activités strictement professionnelles ou s'il relève d'une autre activité. Ainsi, si l'on conçoit que l'échange de correspondance électronique entre travailleurs s'inscrive dans un contexte professionnel, il n'est pas exclu qu'il ne relève pas de l'exercice de tâches professionnelles mais plutôt d'échanges à titre privé. Dans ce cas, ils ne relèvent pas des traitements mis en œuvre par l'employeur.

61 Art. 2, d), de la directive 95/46/CE et art. 4, 7), du RGPD.

L'identification du responsable du traitement n'est pas anodine car elle sera déterminante en matière de responsabilité en cas de violation de la législation de la protection des données. Cette problématique nous permet également de mettre en perspective la situation particulière de l'employeur responsable de traitement : alors qu'il est tenu de faire respecter la législation relative à la protection de la vie privée par ses travailleurs, il ne peut néanmoins s'affranchir des principes définis par cette législation lorsqu'il contrôle l'usage qui est fait du courrier électronique, ce qui constitue un traitement de données dans son chef.

C. – *Le contrôle en tant que traitement de données à caractère personnel*

30. Les opérations de contrôle ou de surveillance de l'utilisation des outils de communication électronique tels que le courrier électronique, Internet ou le téléphone seront mises en œuvre au travers de traitements dès qu'elles impliquent, ne serait-ce que partiellement, l'utilisation de moyens automatisés, ce qui est généralement le cas. Encore faut-il, pour qu'ils tombent dans le champ d'application de la règlementation relative à la protection des données, que ces traitements portent sur des données à caractère personnel.

De l'avis du Groupe de l'Article 29, la surveillance du courrier électronique du travailleur implique bel et bien un traitement de données à caractère personnel. Par contre, le contrôle de l'accès à Internet n'impliquerait pas forcément de traitement de données à caractère personnel. Tel sera le cas lorsque le contrôle est effectué à un niveau si élevé qu'il ne permet pas de lier une personne en particulier à l'accès à certains sites ou modes d'accès ou si seules des données agrégées sont produites[62].

Dans la mesure où le contrôle de l'usage du courrier électronique, d'Internet ou du téléphone constituera effectivement un traitement de données à caractère personnel, il devra être conforme aux principes définis par la règlementation européenne. La présente contribution ne prétend pas offrir une analyse de l'ensemble des conditions de traitement, et en particulier de celles qui pourraient découler du RGDP. Il convient de garder à l'esprit que le RGPD innove sur bien des points par rapport

[62] Groupe de l'Article 29, avis 8/2001 sur le traitement de données à caractère personnel dans le contexte professionnel, 13 septembre 2001, WP 48, p. 14.

à la directive 95/46/CE[63]. Par ailleurs, comme expliqué *supra*, des législations nationales peuvent définir des conditions particulières pour les traitements de données dans ce contexte, de sorte qu'il convient de se reporter aux dispositions de droit interne pour déterminer le régime applicable à un cas particulier.

Nous proposons de nous pencher sur les principes dégagés au niveau européen et qui nous semblent traduire les exigences les plus essentielles de cette règlementation en ce qui concerne l'admissibilité du traitement.

Pour ce qui concerne la protection des données à caractère personnel, il y a à notre connaissance très peu de jurisprudence au niveau européen sur leur application dans le contexte du contrat de travail[64] et en tout cas pas dans le domaine qui fait l'objet de cette contribution à savoir celui du contrôle de l'usage des outils de communication du travailleur par l'employeur. Aussi, il nous semble d'autant plus intéressant de mettre en exergue les principes dégagés par le Groupe de l'Article 29 et au sein du Conseil pour contextualiser les exigences de la règlementation en matière de protection des données au contrôle des communications électroniques.

1. – *Principe de nécessité*

31. Le contrôle ou la surveillance de l'usage du courrier électronique ou d'autres moyens mis à la disposition du travailleur doit être nécessaire.

Nous situons ce critère au niveau de la nécessité de la mise en œuvre du traitement de données. Ainsi, l'employeur devrait-il toujours se poser la question préalable de savoir s'il ne peut atteindre ses objectifs par d'autres moyens de supervision moins intrusifs. C'est en quelque sorte une exigence de subsidiarité qui est à prendre en compte.

Ainsi, le Groupe de l'Article 29 considère-t-il par exemple que l'employeur devrait privilégier la prévention plutôt que la détection en ce

63 Voy. not. l'introduction de l'obligation de désigner un délégué à la protection des données pour certains responsables de traitement et sous-traitants (notamment les autorités publiques ; *cf.* art. 37 du RGPD). Dès lors qu'un tel délégué est désigné, son champ d'action comprendra tous les traitements mis en œuvre, y compris les contrôles des communications du personnel (pour un commentaire sur le sujet, voy. K. ROSIER, « Délégué à la protection des données : une nouvelle fonction, un métier en devenir », in *Vers un droit européen de la protection des données ?*, Bruxelles, Larcier, 2017, p. 140).

64 C.J.U.E. (8e ch.), 19 juin 2014, *Pharmacontinente c. Saúde e Higiene e.a.*, C-683/13 (en matière de contrôle du temps de travail) ; C.J.U.E., 20 mai 2003, *Österreichischer Rundfunk e.a.*, C-465/00, C-138/01 et C-139/01 (divulgation de rémunérations d'employés à une autorité de contrôle).

qui concerne l'utilisation d'Internet en ayant recours, dans la mesure du possible, à des outils techniques verrouillant l'accès à certains sites ou générant des avertissements automatiques[65]. La recommandation du Comité des ministres aux États membres du Conseil de l'Europe va dans le même sens[66].

Nous verrons que dès lors qu'un traitement de données est mis en œuvre, une autre exigence de nécessité s'impose mais au niveau de la sélection des données traitées et de l'adéquation des moyens de traitements au regard de la finalité poursuivie. Cette exigence s'inscrit dans le cadre du principe de proportionnalité[67].

2. – *Principe de finalité*

32. Les données collectées à des fins de contrôle devront en outre toujours l'être pour des finalités déterminées, explicites et légitimes, et sous l'égide la directive 95/46/CE, elle ne peuvent pas être traitées ultérieurement de manière incompatible avec ces finalités[68].

Cette exigence requiert, selon nous, que l'employeur ne se contente pas de considérer le contrôle comme une finalité en soi mais qu'il détermine les finalités du contrôle ou de la surveillance de façon plus précise (par exemple, contrôle du bon fonctionnement du réseau ou un contrôle du respect des directives de l'entreprise concernant l'utilisation du courrier électronique).

Le principe d'interdiction de réutilisation des données implique également que ce n'est pas parce qu'un employeur collecte et conserve des informations pour une finalité de contrôle particulière qu'il peut réutiliser ces informations dans le cadre d'un autre type de contrôle. La Commission et le Groupe de l'Article 29 citent l'exemple suivant : les données collectées afin d'assurer la sécurité, le contrôle ou le bon fonctionnement des systèmes de traitement ne devraient pas être traitées dans le but de contrôler le comportement de chaque travailleur[69]. Le RGPD ouvre cependant la porte à une possible réutilisation des données

65 Groupe de l'Article 29, document de travail concernant la surveillance des communications électroniques sur le lieu du travail, 29 mai 2002, WP 55, p. 24.

66 CM/Rec(2015) 5 du Comité des ministres aux États membres sur le traitement des données à caractère personnel dans le cadre de l'emploi, 1er avril 2015, art. 14.2.

67 Voy. sous-section 5, *infra*.

68 Art. 6, § 1, b), de la directive 95/46/CE.

69 Groupe de l'Article 29, document de travail concernant la surveillance des communications électroniques sur le lieu du travail, 29 mai 2002, WP 55, p. 14 ; « Deuxième phase de consultation des partenaires sociaux sur la protection des données à caractère personnel des travailleurs », *op. cit.*, p. 19.

sous certaines conditions. Il prévoit la possibilité d'une réutilisation moyennant le consentement de la personne concernée pour le traitement de ses données à de nouvelles fins incompatibles et l'hypothèse d'un traitement ultérieur des données à des fins incompatibles basé sur le droit de l'Union ou d'un État membre[70].

Il demeure que la question du consentement reste en tout état de cause particulièrement délicate. Nous y reviendrons sous la section 3.

3. – *Principes de légitimité et de licéité*

33. Les finalités de traitement devront en outre être légitimes, c'est-à-dire ne pas porter une atteinte disproportionnée aux intérêts ou aux libertés et droits fondamentaux de la personne concernée par rapport à l'intérêt que l'employeur peut trouver à contrôler son travailleur. Le respect de cette exigence de proportionnalité appelle donc un équilibre et est sujette à appréciation. Le législateur européen avait néanmoins d'ores et déjà déterminé à l'article 7 de la directive 95/46/CE les six hypothèses dans lesquelles un traitement de données à caractère personnel poursuit *a priori* une finalité légitime. L'employeur ne pouvait effectuer de contrôle ou de surveillance que dans la mesure où il pouvait justifier de l'une de ces bases de légitimité telles que transposées dans la loi nationale applicable. L'entrée en application du RGPD ne change pas fondamentalement la donne dès lors que ces six hypothèses sont maintenues à l'article 6 de ce Règlement même si elles sont désormais associées à un principe de licéité du traitement et ne doivent plus faire l'objet d'une transposition en droit interne.

Parmi ces hypothèses, on en retrouve plusieurs qui peuvent *a priori* offrir une base intéressante à l'employeur : l'exécution d'un contrat, le consentement du travailleur, l'obligation légale et le dernier cas prévu par la directive et reprenant l'existence d'une balance entre intérêts et droits de la personne concernée et intérêt du responsable du traitement.

34. S'il est *a priori* raisonnable de penser à l'hypothèse de l'exécution du contrat de travail pour justifier le contrôle ou la surveillance d'un travailleur, la règlementation exige que le traitement soit *nécessaire* à l'exécution du contrat[71]. Cette base ne nous paraît être pertinente que dans les cas particuliers où l'exécution du contrat de travail implique ou

[70] Art. 6, § 4, du RGPD.
[71] Art. 7, b), de la directive et 6, § 1er, b), du RGPD.

exige effectivement qu'un contrôle ou une surveillance de l'utilisation des outils de communication électronique, de par la nature même des prestations à effectuer. La seule existence de l'autorité de l'employeur sur ses travailleurs conférant au premier un pouvoir de contrôle et de surveillance de la bonne exécution des prestations de travail par les seconds ne nous semble en effet pas impliquer pour autant l'existence d'une *nécessité* d'effectuer un contrôle de l'usage des courriers électroniques, d'Internet ou du téléphone pour assurer cette surveillance.

35. En ce qui concerne le consentement du travailleur, on constatera d'emblée les limites offertes par cette hypothèse. En effet, ce cas de figure ne peut offrir une base de traitement que lorsque seules les données du travailleur sont concernées. Tel ne sera pas le cas de l'utilisation du courrier électronique impliquant un expéditeur ou un destinataire externe dont on n'aura pas obtenu le consentement. De plus, la valeur d'un consentement donné par un travailleur dans le contexte de la relation de travail est mise en cause. Aux termes de l'article 2, h), de la directive 95/46/CE, le « consentement de la personne concernée impliquait une manifestation de volonté, libre, spécifique et informée par laquelle la personne concernée accepte que des données à caractère personnel la concernant fassent l'objet d'un traitement ». Ainsi, par exemple, il ne pouvait se déduire d'une absence de réaction, par exemple du fait ne pas avoir modifié un paramétrage par défaut pour bloquer certains traitements[72].

La possibilité de se prévaloir d'un consentement d'un travailleur libre lorsqu'il est requis dans le cadre d'une relation d'autorité a fait débat. En 2002, la Commission européenne semblait en douter et a considéré que l'employeur devrait éviter de recourir exclusivement au consentement pour légitimer un traitement de données à caractère personnel et devrait pouvoir se fonder sur d'autres motifs légitimes[73]. Cette méfiance reste plus que jamais d'actualité[74]. Le Règlement renforce les exigences pour que le consentement soit véritable et de qualité[75] et le considé-

72 Groupe de l'Article 29, Opinion 2/2017 on Data Processing at Work, WP 249, 8 juin 2017, p. 7.

73 « Deuxième phase de consultation des partenaires sociaux sur la protection des données à caractère personnel des travailleurs », *op. cit.*, pp. 12 et 13. Le Groupe de l'Article 29 considère quant à lui que dans le cadre d'un contrôle du travailleur, si le consentement du travailleur peut entrer en ligne de compte pour déterminer si le traitement satisfait à l'art. 6 de la directive, il ne peut jamais être le facteur déterminant de la légitimité (Groupe de l'Article 29, avis 8/2001 sur le traitement de données à caractère personnel dans le contexte professionnel, 13 septembre 2001, WP 48, p. 24).

74 Voy. en ce sens Groupe de l'Article 29, Opinion 2/2017 on Data Processing at Work, WP 249, 8 juin 2017, p. 6.

75 Art. 7 du RGPD. Voy. pour un commentaire plus détaillé des nouvelles exigences : C. DE TERWANGNE, K. ROSIER et B. LOSDYCK, « Lignes de force du nouveau Règlement relatif à la protection des données à caractère personnel », *R.D.T.I.*, 2016, n° 62, pp. 40-42.

rant 42 précise que « le consentement ne devrait pas être considéré comme ayant été donné librement si la personne concernée ne dispose pas d'une véritable liberté de choix ou n'est pas en mesure de refuser ou de retirer son consentement sans subir de préjudice ». Précisément, lorsqu'un travailleur peut craindre soit de ne pas être engagé, soit de subir des mesures de représailles s'il refuse ou retire un consentement, on peut douter de l'existence de l'espace indispensable à l'exercice de cette liberté.

C'est d'ailleurs ce que pointe le Groupe de l'Article 29 dans un document du 8 juin 2017[76]. Il souligne que dans la majorité des cas la relation de dépendance qui caractérise la situation du travailleur vis-à-vis de son employeur constitue un obstacle à ce qu'il puisse librement accepter ou refuser, voire encore révoquer un consentement donné. Il en déduit qu'il ne peut s'agir d'un fondement juridique du traitement, sauf lorsqu'aucune conséquence ne peut résulter de l'acception ou du refus d'une offre faite à un travailleur[77]. La question de la possibilité d'un consentement véritable pose donc question. Par ailleurs, même à supposer qu'un employeur puisse démontrer que le consentement obtenu est conforme aux exigences du Règlement, ce dernier explicite le fait que le consentement peut être retiré à tout moment, avec pour conséquence que le traitement ne peut être poursuivi après ce retrait. On comprend que ce revers serait particulièrement problématique dans le cadre d'une politique de surveillance[78].

36. Si le critère de la nécessité du respect d'une obligation légale à laquelle le responsable du traitement est soumis peut offrir ponctuellement une base pour effectuer un traitement, l'employeur devra bien souvent se rabattre sur celui fondé sur son intérêt légitime. Celui-ci requiert que le traitement soit nécessaire à la réalisation de l'intérêt légitime poursuivi par le responsable du traitement ou par le ou les tiers auxquels les données sont communiquées, à condition que ne prévalent pas l'intérêt ou les droits et libertés fondamentaux de la personne concernée.

Le bénéfice de cette base de justification appelle donc une balance d'intérêts qui doit être effectuée au cas par cas. Le raisonnement à tenir pour effectuer ce type d'exercice a été explicité par le Groupe de l'Article 29 dans un document de travail de 2014[79]. Le responsable du

76 Groupe de l'Article 29, Opinion 2/2017 on Data Processing at Work, WP 249, 8 juin 2017.
77 *Ibid.*, p. 23.
78 Art. 7, § 3, du RGPD.
79 Groupe de l'Article 29, Opinion 06/2014 on the Notion of Legitimate Interests of the Data Controller under Article 7 of Directive 95/46/EC, 9 avril 2014, WP 217, pp. 23 et s.

traitement doit à tout le moins pouvoir justifier d'un intérêt légitime. Cet intérêt doit être compris comme un « enjeu » distinct de la notion de finalité qui, elle, désigne l'objectif que poursuit un responsable de traitement. Ainsi, dans le contexte de la surveillance de communications de travailleurs, l'intérêt pourrait être par exemple d'assurer la sécurité d'un système informatique ou encore de préserver les intérêts économiques de l'entreprise (lutter contre la fuite d'informations confidentielles ou la fraude au temps de travail, c'est-à-dire le fait pour un travailleur de ne pas consacrer son temps de travail à l'exécution de celui-ci). La finalité serait quant à elle la mise en place de mesures permettant tel ou tel contrôle spécifique.

L'intérêt doit par ailleurs être *légitime,* ce qui implique à tout le moins qu'il ne soit pas en contradiction avec la loi, qu'il s'agisse d'un intérêt actuel (présent et non hypothétique) et suffisamment précis que pour que l'on puisse effectuer une mise en balance avec les intérêts des personnes concernées[80]. Le Groupe de l'Article 29 identifie, entre autres, comment peuvent être considérées comme relevant d'un intérêt *a priori* légitime la surveillance des travailleurs pour des raisons de sécurité ou de management, la mise en place d'une procédure de lancement d'alertes (*whistleblowing*) ou encore la sécurisation des lieux et des systèmes informatiques et de communication[81].

Dès lors que l'intérêt du responsable du traitement est identifié, il convient de vérifier quels sont les intérêts des personnes concernées qui pourraient être impactés par le traitement de données. Le Groupe de l'Article 29 prône à cet égard une interprétation large de la notion d'intérêt, non limitée aux droits et libertés fondamentaux[82]. Il n'est pas non plus exigé que les intérêts soient *légitimes* dans le sens où les personnes dont les données font l'objet d'un traitement ne perdent pas le bénéfice de toute protection du simple fait qu'elles ont commis une faute, voire une infraction pénale. Ainsi, un travailleur ne perd pas toute protection parce qu'on le soupçonne d'être à l'origine d'une divulgation fautive de secrets d'affaires à un tiers.

Tout est affaire de proportionnalité. Le Groupe de l'Article 29 préconise d'ailleurs qu'une fois identifiés les intérêts du responsable de traitement et ceux des personnes concernées, il soit vérifié si des mesures sont susceptibles d'être prises par le responsable de traitement pour

80 *Ibid.*, p. 25.
81 *Ibid.*, p. 25.
82 *Ibid.*, pp. 29 et 30.

aménager un juste équilibre qui permette d'atténuer l'impact sur les intérêts des personnes lorsque les intérêts en présence le commandent. Cet exercice appelle également la prise en compte notamment des techniques de traitements utilisées.

C'est d'ailleurs l'évolution des technologies permettant des traitements plus nombreux et à moindre coût qui a amené le Groupe de l'Article 29 à adopter un document en juin 2017 dans lequel il propose des balises pour cette balance d'intérêts au regard de ces nouvelles technologies[83]. Tout en ne modifiant pas fondamentalement les intérêts en présence, la mise en œuvre de ces technologies est susceptible d'avoir un plus grand impact sur les droits des personnes. Par exemple, si au lieu de se limiter à installer un système anti-virus pour protéger le réseau informatique, l'employeur décide d'utiliser des techniques de *screening* plus sophistiquées des communications, cela peut avoir un impact plus grand sur le secret des communications dont bénéficient les travailleurs. Pour en atténuer l'impact, l'employeur pourrait, par exemple, limiter le *screening* à certaines communications ou offrir des alternatives de moyens de communications via des boîtes mail distinctes. Cet examen est à réaliser au cas par cas et peut amener à un exercice d'analyse d'impact que le Règlement prévoit pour certains traitements[84].

La recherche de cet équilibre devra également intégrer une dimension proactive que suppose le respect du principe-clé d'« *accountability* » qui est désormais inscrit à l'article 5, paragraphe 2, du RGPD[85]. Le responsable du traitement, comme sous le régime de la directive 95/46/CE, est tenu de respecter les principes du traitement mais il est désormais spécifié qu'il doit démontrer que ceux-ci sont respectés[86]. C'est ce que désigne ce « principe de responsabilité », entendu non pas comme impliquant essentiellement une obligation de réparer le dommage en cas de violation de la réglementation[87], mais qui s'apparente davantage à l'idée de « répondre de », en l'occurrence répondre des mesures prises pour s'assurer du respect de la règlementation (le concept étant mieux traduit par le terme anglais d'« *accountability* », distinct de celui de « *liability* » qui subsiste par ailleurs). Cela suppose donc une certaine proactivité et anticipation des critiques que

83 Groupe de l'Article 29, Opinion 2/2017 on Data Processing at Work, WP 249, 8 juin 2017, pp. 3 et 4.
84 Art. 35 du RGPD.
85 Voy. pour un commentaire plus détaillé : C. DE TERWANGNE, K. ROSIER et B. LOSDYCK, « Lignes de force du nouveau Règlement relatif à la protection des données à caractère personnel », *op. cit.*, p. 28.
86 Art. 5, § 2, du RGPD.
87 Comparez avec l'art. 23 de la directive intitulé « responsabilité ».

l'on pourrait formuler à l'égard d'un traitement. Ce principe général d'*accountability* applicable à tout traitement prend corps avec des obligations particulières pour certains types de traitements ou responsables de traitement, qui formalisent les mesures à prendre par le responsable du traitement pour s'assurer du respect des principes de protection, telles les exigences de protection des données dès la conception et de protection des données par défaut qui sont imposées par le Règlement.

4. – *Principe de transparence*

37. Il s'agit, à notre estime, d'une exigence essentielle, en particulier dans le contexte qui nous occupe. En effet, il permet une forme d'anticipation du travailleur sur la façon dont il doit se comporter dans un environnement numérique. Par ailleurs, dans un contexte où la technologie permet une surveillance plus discrète (par exemple par un logiciel enregistrant automatiquement des copies d'écran du travailleur) et une réutilisation de données, il est indéniable que seule une information complète et aisément accessible permettra à la personne dont les données sont ainsi traitées de se rendre compte des moyens de surveillance mis en œuvre[88].

Tant la directive 95/46/CE que le RGPD exigent que le traitement soit transparent. Cela se traduit essentiellement par l'obligation d'information préalable[89]. Le contrôle ne peut donc être secret mais doit, au contraire, faire l'objet d'une information préalable destinée aux travailleurs. Ainsi, le Groupe de l'Article 29 estime-t-il qu'un employeur pourrait avoir un intérêt légitime à contrôler les performances de ses travailleurs en évaluant leurs prestations à l'aide d'ordinateurs (par exemple, surveiller le temps qu'un travailleur a passé à dactylographier, le nombre de fichiers enregistrés, l'heure à laquelle il a allumé et éteint son ordinateur, etc.) pour autant que les travailleurs en aient été informés. Par contre, si cette surveillance a été réalisée à l'insu du personnel, le traitement des données des travailleurs est en contradiction avec les dispositions de la directive 95/46/CE[90].

Concrètement, cette exigence de transparence ne nous semble pas requérir une information *ad hoc* lors de chaque contrôle effectué mais pourrait se traduire par une information générale et préalable

88 Groupe de l'Article 29, Opinion 2/2017 on Data Processing at Work, WP 249, 8 juin 2017, pp. 4 et 8.
89 Que l'on retrouve définie aux art. 10 et 11 de la directive 95/46/CE et 12 à 14 du RGPD.
90 Groupe de l'Article 29, avis 8/2001 sur le traitement de données à caractère personnel dans le contexte professionnel, 13 septembre 2001, WP 48, p. 27.

communiquée aux travailleurs. C'est d'ailleurs l'avis du Groupe de l'Article 29 qui précise que l'obligation de transparence dans ce contexte se traduit par une obligation de fournir à son personnel une déclaration claire, précise et aisément accessible de sa politique relative à la surveillance du courrier électronique et de l'utilisation d'Internet[91].

Le contenu de l'information doit être conforme aux exigences des dispositions de la règlementation et, tout en avisant de la possibilité des contrôles effectués par l'employeur, il doit préciser leurs finalités ainsi que fournir toute autre information qui s'avère nécessaire pour assurer la loyauté du traitement. Dans ce cadre, il pourrait être exigé d'informer les travailleurs sur les circonstances, modalités et portée du contrôle ou de la surveillance et d'identifier les personnes chargées de les effectuer par référence à leur fonction par exemple, ainsi que les personnes susceptibles de recevoir communication de ces informations. Si l'on a égard au Règlement, celui-ci renforce encore l'obligation d'information en imposant des exigences tendant à une information à la fois plus complète[92] et de meilleure qualité[93] pour qu'elle soit compréhensible et accessible pour les destinataires.

Dans sa recommandation du 1er avril 2015, le Comité des ministres aux Etats membres du Conseil de l'Europe prône « [u]ne description particulièrement claire et complète des catégories de données à caractère personnel qui peuvent être collectées au moyen de TIC »[94].

L'objectif est que les travailleurs concernés soient informés à la fois des données qui sont conservées et pour quelles durées ainsi que les finalités de traitement.

Le Groupe de l'Article 29 avait quant à lui dès 2002 recommandé la communication des informations suivantes[95] :

– Les lignes directrices de l'entreprise concernant l'utilisation du courrier électronique décrivant dans le détail dans quelle mesure les systèmes de communication de l'entreprise peuvent être utilisés à des

91 Groupe de l'Article 29, document de travail concernant la surveillance des communications électroniques sur le lieu du travail, 29 mai 2002, WP 55, pp. 14 et 15.

92 Règlement, art. 13. Il est par exemple question d'informations qui selon les cas de figure peuvent avoir trait à la base juridique sur lesquelles repose le traitement de données, à la source d'où proviennent les données si celles-ci n'ont pas été collectées directement auprès de la personne concernée ou encore à l'intention de transférer les données à caractère personnel vers un pays tiers ou à une organisation internationale.

93 Art. 12, § 1, du RGPD. Il est question d'une communication concise, transparente, compréhensible et aisément accessible, en des termes clairs et simples.

94 CM/Rec(2015) 5 du Comité des ministres aux États membres sur le traitement des données à caractère personnel dans le cadre de l'emploi, 1er avril 2015, art. 10.3.

95 Groupe de l'Article 29, document de travail concernant la surveillance des communications électroniques sur le lieu du travail, 29 mai 2002, WP 55, pp. 15, 22 et 25.

fins privées ou personnelles par les salariés (par exemple les limites concernant les périodes et la durée d'utilisation) ; concernant l'usage du courrier électronique, le Groupe de l'Article 29 recommande également que l'employeur indique si le travailleur est ou non autorisé à disposer d'un compte de courrier électronique à usage strictement personnel, si l'utilisation de comptes de messagerie Web est autorisée sur le lieu de travail et si l'employeur recommande à son personnel l'utilisation d'un compte privé de messagerie Web pour utiliser le courrier électronique à des fins strictement personnelles. En ce qui concerne la consultation d'Internet, le Groupe de l'Article 29 invite les employeurs à préciser si, le cas échéant, certains éléments ne peuvent être visualisés ou copiés ;

– Les motifs et les finalités de l'éventuelle mise en place d'une surveillance ;
– Des informations détaillées sur les mesures de surveillance prises (qui surveille, quand et comment) ; quant à l'usage d'Internet, le Groupe de l'Article 29 considère que les travailleurs doivent être informés des systèmes installés pour empêcher l'accès à certains sites ou pour détecter une éventuelle utilisation abusive ;
– Des informations détaillées sur les procédures d'application précisant comment et quand les travailleurs seront avertis en cas d'infraction aux lignes directrices internes et pourront réagir dans un tel cas. Le Groupe de l'Article 29 recommande que l'employeur informe immédiatement le travailleur d'un quelconque abus des communications électroniques détecté, sauf si des raisons impérieuses justifient la poursuite de la surveillance ;
– La durée de conservation des éventuelles copies de sauvegarde des messages et le moment où les messages électroniques sont définitivement effacés du serveur ;
– Les mesures de sécurité en place ;
– L'implication éventuelle des représentants des travailleurs dans la mise en place de la politique de contrôle et de surveillance.

Une autre manière, complémentaire à une information individuelle, de mettre en œuvre ce principe de transparence est de soumettre aux représentants des travailleurs la politique de contrôle que l'employeur entend mettre en place. Cette communication et discussion préalables avec des organisations représentatives des travailleurs peuvent d'ailleurs s'avérer obligatoires en exécution de la directive 2002/14/CE relative à

la consultation des travailleurs[96] qui prévoit une obligation d'informer et de consulter les salariés concernant les décisions susceptibles d'entraîner des changements importants dans l'organisation du travail.

Soulignons que ce principe d'information préalable ne va pas toutefois pas sans soulever quelque opposition. Il ressort tant des besoins exprimés par les partenaires sociaux consultés que des considérations du Groupe de l'Article 29 qu'une surveillance secrète devrait, dans certaines circonstances, être admise[97]. Ainsi, la Commission envisageait-elle de permettre une surveillance secrète en cas de soupçon raisonnable d'une activité criminelle ou d'un autre acte répréhensible dans le chef d'un travailleur[98]. Or l'article 10 de la directive 95/46/CE (pas plus que les articles 12 à 14 du RGPD) ne prévoit pas d'exception sur laquelle pourrait se fonder l'employeur pour effectuer une surveillance secrète. Les États membres avaient néanmoins la possibilité, en vertu de l'article 13, g), de la directive, de prendre des mesures législatives visant à limiter la portée des obligations prévues à l'article 10 lorsqu'une telle limitation constitue une mesure nécessaire pour sauvegarder la protection des droits et libertés d'autrui. Cette possibilité est maintenue à l'article 23 du Règlement mais avec une nouveauté toutefois : si les dérogations doivent toujours résulter d'une mesure législative, le Règlement imposera que le texte adopté contienne des spécifications minimum concernant des aspects du traitement, spécifications dont certaines sont assez classiques (les finalités du traitement ou des catégories de traitement, les catégories de données à caractère personnel, l'étendue des limitations introduites, etc.) et d'autres plus novatrices (les garanties destinées à prévenir les abus ou l'accès ou le transfert illicites ou encore les risques pour les droits et libertés des personnes concernées, ce dernier point ne manquant pas de poser question quant à la manière dont il pourra être mis en œuvre dans une loi).

En tout état de cause, il ne nous paraît pas nécessaire de permettre un contrôle secret. En effet, à partir du moment où l'on admet que l'obligation d'information peut être accomplie par la communication d'une information préalable adressée à tous les employés, il est parfaitement envisageable d'y décrire les modalités de contrôle qui seront appliquées

96 Directive 2002/14/CE du Parlement européen et du Conseil du 11 mars 2002 établissant un cadre général relatif à l'information et la consultation des travailleurs dans la Communauté européenne.

97 Groupe de l'Article 29, document de travail concernant la surveillance des communications électroniques sur le lieu du travail, 29 mai 2002, WP 55, p. 15.

98 « Deuxième phase de consultation des partenaires sociaux sur la protection des données à caractère personnel des travailleurs », *op. cit.*, p. 19.

dans le cadre d'un soupçon d'une activité criminelle dans le chef d'un travailleur.

5. – *Principe de proportionnalité*

38. Les données collectées doivent être adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont collectées et pour lesquelles elles sont traitées ultérieurement. Ce principe conduit à limiter les données qui peuvent être collectées et traitées de différentes manières[99]. Cette limitation peut situer en effet sur plusieurs plans : géographique (uniquement certains lieux, tel le lieu sur lequel le travailleur est censé prester), temporel (uniquement pendant les heures normales de travail) ou encore par rapport aux données (différencier les modalités d'accès lors d'un contrôle selon que le fichier concerné est professionnel ou qu'il a été enregistré dans un fichier qualifié de « privé »)[100].

On aura égard aux modalités de contrôle admissibles au regard des finalités poursuivies. Ainsi le Groupe de l'Article 29 considère-t-il que si des employeurs pourraient être autorisés à contrôler les données relatives au trafic (adresses de site consultés, temps et durée des connexion, destinataires de courriers électroniques), ils ne peuvent certainement pas en principe accéder au contenu des communications électroniques de leurs travailleurs[101]. Il estime également qu'une utilisation abusive d'Internet peut dans bien des cas être établie sans examiner le contenu des sites consultés[102]. Il est cependant indéniable que dans certaines hypothèses, il est impossible de réaliser le but poursuivi sans prendre connaissance du contenu d'une communication ou que l'absence de prise de connaissance du contenu pourrait obliger l'employeur à se contenter de simples suspicions. Ainsi, la prévention de certains comportements illicites, tels que la diffamation ou encore la communication d'images pédophiles, ne pourra être assurée efficacement sans la possibilité de prendre connaissance du contenu des communications suspectes.

99 Il découlait de l'art. 6, § 1, c), de la directive 95/46/CE et est repris à l'art. 5, § 1, c), du RGPD sous le vocable « principe de minimisation des données ».

100 Groupe de l'Article 29, Opinion 2/2017 on Data Processing at Work, WP 249, 8 juin 2017, pp. 7 et 8.

101 Groupe de l'Article 29, avis 8/2001 sur le traitement de données à caractère personnel dans le contexte professionnel, 13 septembre 2001, WP 48, p. 34 ; Groupe de l'Article 29, document de travail concernant la surveillance des communications électroniques sur le lieu du travail, 29 mai 2002, WP 55, p. 14.

102 Groupe de l'Article 29, document de travail concernant la surveillance des communications électroniques sur le lieu du travail, 29 mai 2002, WP 55, p. 24.

Une autre implication de ce principe de proportionnalité s'exprime dans l'admission ou non du caractère continu du contrôle et de la surveillance. La collecte continue d'informations sur le trafic des courriers électroniques sera plus aisément admissible à des fins de bonne administration et de protection du réseau que pour s'assurer que les travailleurs ne commettent pas d'actes répréhensibles, finalité dont on estime qu'elle n'appelle qu'un contrôle ponctuel. La Commission suggère de n'autoriser la surveillance *continue* que pour des raisons de santé, de sécurité, de sûreté ou de protection des biens de l'entreprise[103].

Le principe prévaut également en ce qui concerne les contrôles collectifs et individualisés : le caractère général ou individualisé des contrôles doit être justifié au vu de la finalité poursuivie. La Commission note que : « sauf dans certains cas, par exemple dans le cadre d'une surveillance automatisée visant à assurer la sécurité et le bon fonctionnement du système (par exemple, pour le protéger contre les virus), la surveillance systématique de l'utilisation du courrier électronique ou d'Internet par chaque travailleur devrait être interdite. Une surveillance individuelle pourrait être effectuée lorsqu'une activité criminelle, un acte répréhensible ou un manquement *grave*[104] peut *raisonnablement*[105] être soupçonné(e), à condition qu'il n'existe aucun autre moyen moins indiscret d'atteindre le résultat souhaité (par exemple, la surveillance objective du trafic de données plutôt que du contenu des messages électroniques, l'utilisation préventive de la technologie, etc.) ».

Dans un même ordre d'idées, les données ne pourront être conservées sous une forme permettant l'identification des personnes concernées pendant une durée qui excéderait celle nécessaire à la réalisation des finalités de contrôle pour lesquelles elles sont collectées[106].

Dans sa recommandation du 1er avril 2015, le Comité des ministres aux États membres du Conseil de l'Europe adopte une position très tranchée concernant le contrôle de communications privées. Il préconise qu'« [e]n aucun cas le contenu, l'envoi et la réception de communications électroniques privées dans le cadre du travail ne devraient faire l'objet d'une surveillance ».[107] Il demeure toutefois parfois difficile de faire le

103 « Deuxième phase de consultation des partenaires sociaux sur la protection des données à caractère personnel des travailleurs », *op. cit.*, p. 19.
104 Souligné par l'auteur.
105 Souligné par l'auteur.
106 Comme exigé à l'art. 7, § 1, e), de la directive 95/46/CE et repris à l'art. 5, § 1, e), du RGPD sous le vocable « principe de limitation de la conservation ».
107 CM/Rec(2015) 5 du Comité des ministres aux États membres sur le traitement des données à caractère personnel dans le cadre de l'emploi, 1er avril 2015, art. 14.4.

partage entre communication privée et communication professionnelle, même si l'on comprend aux travers des réticences exprimées que la préoccupation est qu'on évite une surveillance des communications qui n'ont aucune incidence sur le contrat de travail par un employeur qui en aurait la possibilité sur le plan technique.

6. – *L'interdiction de traiter des données « sensibles »*

39. Il n'est pas exclu que le contrôle exercé implique le traitement de données à caractère personnel dites « sensibles » ou selon la terminologie du RGPD « particulières ». Il s'agit de données qui révèlent l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques, l'appartenance syndicale, les données relatives à la santé et à la vie sexuelle ainsi que les données judiciaires[108]. Il en serait par exemple ainsi du contenu de courriers électroniques interceptés concernant l'appartenance politique ou syndicale du travailleur. Dans l'affaire *Bărbulescu* tranchée par la Cour européenne des droits de l'homme il était question de propos échangés qui concernaient la vie sexuelle du travailleur[109].

Le traitement des données sensibles était en principe interdit en vertu de l'article 8 de la directive 95/46/CE. Le traitement n'était autorisé que dans le cadre d'exceptions prévues dans les législations nationales. Le régime reste quasiment identique sous l'égide du RGPD[110].

Ce traitement soulève dès lors une première difficulté : l'employeur doit pouvoir se prévaloir d'une des hypothèses prévues dans la règlementation applicable. Parmi celles qui y sont reprises pour ce qui concerne les données sensibles autres que judiciaires[111], trois nous semblent plus pertinentes en ce concerne le cas du contrôle exercé par l'employeur sur ses travailleurs.

Tout d'abord le traitement est possible avec le consentement des personnes concernées[112]. Toutefois, comme nous l'avons signalé ci-avant, la possibilité d'un consentement libre dans le cadre d'une relation de travail est fortement mise en cause. Par ailleurs, dès que la communication

108 C'est-à-dire les données relatives aux infractions et aux condamnations pénales ou aux mesures de sûreté connexes.

109 Voy. *supra*, section II.

110 Règlement, art. 9 et 10. L'art. 9 inclut dans ce régime de nouveaux types de données : les données génétiques et biométriques.

111 Nous ne traiterons pas de ces données dès lors que la règlementation renvoie à des conditions qui sont à définir par le droit interne et qui varient d'un État membre à l'autre.

112 Art. 8, § 2, a), de la directive 95/46/CE et 9, § 1, a), du RGPD.

concerne une personne externe à l'entreprise, il devient illusoire de vouloir obtenir son consentement.

La règlementation prévoit également la possibilité de traiter des données sensibles lorsque le traitement est nécessaire aux fins de respecter les obligations et les droits spécifiques du responsable du traitement en matière de droit du travail, dans la mesure où il est autorisé par une législation nationale prévoyant des garanties adéquates[113]. L'applicabilité de cette exception exige donc que l'employeur soit autorisé ou tenu d'effectuer le traitement des données sensibles dans le cadre de son activité de contrôle des travailleurs, ce qui nous semble peu probable. Il reste que tant la directive 95/46/CE et le RGPD permettent par ailleurs aux États membres peuvent prévoir, pour un motif d'intérêt public important[114].

Une seconde difficulté inhérente à cette problématique est que l'employeur ignore bien souvent quel type de données le contrôle et/ou la surveillance effectué(e)(s) peut l'amener à collecter. Cela signifie que dans nombre de cas, l'employeur ne pourra déterminer à l'avance qu'il ne collectera et ne traitera que des données non sensibles et que le caractère sensible ou non des données obtenues ne sera révélé qu'au cours du contrôle effectué. Il en résulte que si l'employeur peut se prévaloir d'une des causes de justification prévue dans la règlementation pour le traitement des données non sensibles mais non d'une exception lui permettant de traiter des données sensibles, il se trouve face à un problème pratique difficilement surmontable.

Cette même impossibilité d'effectuer une sélection préalable des données traitées dans le cadre d'un contrôle entraîne une autre conséquence : le régime le plus strict devrait s'appliquer au traitement de toutes les données. Ainsi la possibilité d'être amené à prendre connaissance de données relatives à la santé oblige l'employeur à respecter les garanties posées par la législation nationale pour traiter ce type de données, par exemple la supervision du traitement par un praticien de la santé. Reconnaissant le problème, le Groupe de l'Article 29 plaide pour que le simple fait que le traitement puisse impliquer inévitablement certaines données sensibles n'empêche ou ne complique sérieusement les activités de surveillance par ailleurs légitimes[115].

113 Art. 8, § 2, b), de la directive 95/46/CE et 9, § 1, b), du RGPD.
114 Art. 8, § 4 de la directive 95/46/CE et 9, § 1, g), du RGPD.
115 Groupe de l'Article 29, document de travail concernant la surveillance des communications électroniques sur le lieu du travail, 29 mai 2002, WP 55, p. 17.

Ces difficultés impliquent selon nous la plus grande prudence dans la manière dont les contrôles sont mis en œuvre et plaident également pour l'adoption de moyens de contrôle collectant le minimum de données.

7. – *L'interdiction de décisions automatisées*

40. La règlementation prévoit l'interdiction des décisions individuelles automatisées. Il s'agit de l'expression d'une défiance face à la « machine » pour éviter que des décisions significatives ne soient prises sans intervention d'un jugement humain. La directive reconnaissait à toute personne « le droit de ne pas être soumise à une décision produisant des effets juridiques à son égard ou l'affectant de manière significative, prise sur le seul fondement d'un traitement automatisé de données destiné à évaluer certains aspects de sa personnalité, tels que son rendement professionnel, son crédit, sa fiabilité, son comportement, etc. »[116]. Le contexte professionnel était clairement visé.

Le RGPD renforce encore cette protection et intègre dans le mécanisme de décision automatisée une autre notion : celle du profilage[117]. Par profilage, on entend désigner « toute forme de traitement automatisé de données à caractère personnel consistant à utiliser ces données à caractère personnel pour évaluer certains aspects personnels relatifs à une personne physique, notamment pour analyser ou prédire des éléments concernant le rendement au travail, la situation économique, la santé, les préférences personnelles, les intérêts, la fiabilité, le comportement, la localisation ou les déplacements de cette personne physique »[118]. L'article 22 du RGPD reconnaît à la personne concernée « le droit de ne pas faire l'objet d'une décision fondée exclusivement sur un traitement automatisé, y compris le profilage, produisant des effets juridiques la concernant ou l'affectant de manière significative de façon similaire ».

Un employeur ne peut donc pas prendre une décision fondée uniquement sur un traitement automatisé de données et, en application du RGPD, d'un traitement automatisé consistant à profiler la personne. Cela peut concerner un contrôle destiné à analyser le rendement de la personne au travail au travers de l'utilisation d'outils de communication, par exemple.

116 Directive 95/46/CE, art. 15.
117 Voy. également à ce sujet : Groupe de l'Article 29, Advice on Essential Elements of a Definition and a Provision on Profiling Within the EU General Data Protection Regulation, 13 mai 2013.
118 Art. 4, 4), du RGPD.

Il existe des exceptions à cette interdiction et celles-ci sont en passe d'évoluer puisque le RGPD les reformule et les complète en ajoutant une hypothèse, celle du consentement de la personne concernée. Ainsi, moyennant des garanties supplémentaires, une décision automatisée ne pourrait être envisagée que lorsque la décision est (i) nécessaire à la conclusion ou à l'exécution d'un contrat entre la personne et le responsable du traitement, (ii) autorisée par une disposition légale qui prévoit également des mesures appropriées pour la sauvegarde des droits et libertés et des intérêts légitimes de la personne concernée ou encore (iii) fondée sur un consentement spécifique de la personne concernée.

Aussi, lorsqu'il est question de mettre en place des contrôles impliquant des décisions automatisées (tels un refus d'accès à tel programme, l'octroi ou le refus d'une rémunération…), il convient de vérifier si la décision est susceptible de produire des effets juridiques ou d'affecter de manière significative de façon similaire la personne concernée. Ainsi, on peut concevoir que l'accès à un système informatique soit entièrement automatisé (octroi d'un *login* et d'un mot de passe à introduire par l'utilisateur à défaut de quoi l'accès n'est pas donné) n'entre pas dans ces cas de figure dès lors que cela n'affecte pas de manière significative la personne concernée. Il en irait différemment s'il s'agissait de conditionner par exemple l'octroi d'une promotion aux temps de connexions à un outil de travail (par exemple, connexion à distance). Il est à remarquer que si la décision automatisée n'est pas nécessaire à la conclusion ou à l'exécution du contrat, ni prévue par la loi, le seul fondement possible est le consentement. Cela compromet la mise en place de ce genre de mécanisme, dans la mesure chaque travailleur peut refuser ou retirer à tout moment son consentement, empêchant ainsi le recours à la décision automatisée.

D. – *Conclusions*

41. La législation en matière de protection des données offre sans doute le cadre le plus adapté à la recherche d'un équilibre lorsqu'il s'agit de la mise en place du contrôle de communications électroniques. Il traduit, au travers de ses dispositions, des exigences de transparence, de finalité légitime et de proportionnalité, mais ne s'y limite pas. Il oblige à une réflexion au moment de la mise en place d'une telle politique afin d'identifier si le traitement envisagé est conforme à la réglementation et intègre également d'autres préoccupations que nous n'avons pas évoquées en matière de sécurité des données.

Ce cadre est en revanche souvent perçu comme complexe surtout lorsqu'il doit être mis en œuvre par de plus petites structures, pas toujours armées pour maîtriser le sujet. Il n'est, pour la même raison, pas toujours mobilisé en jurisprudence, d'autant que ce sont souvent les juridictions du travail qui sont bien souvent saisies de la problématique en première ligne et non un juge spécialisé en la matière. Cela pourrait changer si les autorités de contrôle nationales se voient saisies de ces questions dans le cadre de plaintes avec les nouvelles compétences qu'elles reçoivent pour donner des injonctions aux responsables du traitement[119].

Ceci étant, ces règles restent à combiner avec celles qui touchent au traitement des données de communications électroniques. Nous verrons que des incertitudes pèsent encore sur l'incidence que cette règlementation a ou aura sur la matière.

IV. Le secret des communications électroniques

A. – *Introduction*

42. Le droit à la protection des communications est inscrit à l'article 7 de la Charte des droits fondamentaux de l'Union européenne. Les communications électroniques sont régies par un cadre de règlementation spécifique qui se situe à la croisée de deux pans de la législation : la protection des données et les services des communications électroniques.

La directive 2002/58/CE[120], modifiée quelques années plus tard par la directive 2009/136/CE[121], faisait partie d'un paquet de cinq directives et d'une décision destiné à réformer le cadre réglementaire régissant les services et réseaux de communications électroniques dans l'Union européenne.

119 C. DE TERWANGNE, K. ROSIER et B. LOSDYCK, « Lignes de force du nouveau Règlement relatif à la protection des données à caractère personnel », *op. cit.*, pp. 50 et s.

120 Directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive vie privée et communications électroniques). Cette directive remplace la directive 97/66/CE du 15 décembre 1997 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des télécommunications.

121 Directive modifiant la directive (CE) n° 2002/22 concernant le service universel et les droits des utilisateurs au regard des réseaux et services de communications électroniques, la directive (CE) n° 2002/58 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques et le règlement (CE) n° 2006/2004 relatif à la coopération entre les autorités nationales chargées de veiller à l'application de la législation en matière de protection des consommateurs.

Résolument ancrée dans cette règlementation sectorielle auquel elle emprunte des définitions de concepts clés de son régime juridique, la directive constitue, dans le même temps, une réglementation spécifique qui complétait la directive 95/46/CE pour ce qui concerne les traitements effectués dans le cadre de la fourniture de services de communications électroniques accessibles au public sur les réseaux publics de communications dans l'Union. Nous verrons que cela a une incidence sur la portée des dispositions prévues en matière de secret des communications.

43. Cette règlementation est en passe d'être modifiée. Une proposition de règlement *ePrivacy* a été publiée le 10 janvier 2017[122], qui est censé à terme remplacer ces directives. Le texte étant, à l'heure où nous rédigeons cette contribution, toujours en discussion et susceptible de modifications, nous n'en évoquerons que les grandes tendances sans garantie que celles-ci soient maintenues dans le texte définitif[123].

Notre propos se limitera à la question du secret des communications électroniques dans la mesure où elle peut avoir une incidence sur le contrôle des communications électroniques dans le contexte de la relation de travail. Nous nous proposons de brosser les grandes lignes de la règlementation telle qu'elle existe en soulignant les modifications qui sont proposées ou suggérées. Nous devrons constater qu'il est difficile de prévoir ce qu'impliquera le secret des communications dans les années à venir en raison de plusieurs éléments liés aux difficultés d'interprétation de la portée des textes, d'une part, et à la marge de manœuvre laissée aux États membres, d'autre part.

B. – *Incertitudes quant à la portée de l'interdiction de la surveillance et de l'interception de communications électroniques*[124]

44. Le premier paragraphe de l'article 5 de la directive 2002/58/CE prévoit que « les États membres garantissent, par la législation nationale,

[122] Proposition de Règlement du parlement européen et du Conseil concernant le respect de la vie privée et la protection des données à caractère personnel dans les communications électroniques et abrogeant la directive 2002/58/CE (règlement « vie privée et communications électroniques »), COM(2017) 10 final.

[123] La proposition a d'ailleurs fait l'objet de plusieurs avis qui préconisent des améliorations du texte, que ce soit à l'initiative du Contrôleur européen de la protection des données (avis 6/2017 sur la proposition de règlement relatif à la vie privée et aux communications électroniques [le règlement « vie privée et communications électroniques »]) ou du Groupe de l'Article 29 (Opinion 01/2017 on the Proposed Regulation for the ePrivacy Regulation, 4 avril 2017, WP 247, 2002/58/EC).

[124] Pour une analyse plus détaillée de la proposition de règlement *ePrivacy* et dont la présente section s'inspire, voy. K. ROSIER, « La notion de "donnée à caractère personnel" a-t-elle encore un sens dans la protection des données de communications électroniques ? », in *Law, Norms and Freedom in Cyberspace. Droit, normes et libertés dans le cybermonde : liber amicorum Yves Poullet*, Bruxelles, Larcier, 2018, pp. 699-714.

la confidentialité des communications effectuées au moyen d'un réseau public de communications et de services de communications électroniques accessibles au public, ainsi que la confidentialité des données relatives au trafic y afférentes. En particulier, ils interdisent à toute autre personne que les utilisateurs d'écouter, d'intercepter, de stocker les communications et les données relatives au trafic y afférentes, ou de les soumettre à tout autre moyen d'interception ou de surveillance, sans le consentement des utilisateurs concernés sauf lorsque cette personne y est légalement autorisée conformément à l'article 15, paragraphe 1 »[125]. Il est cependant immédiatement précisé que « le présent paragraphe n'empêche pas le stockage technique nécessaire à l'acheminement d'une communication, sans préjudice du principe de confidentialité ».

45. Le fait que la matière soit régulée dans un texte qui est lié à un secteur a une incidence sur son champ d'application. Tant les directives 2002/58/CE et 2009/136/CE précitées que la proposition de règlement *ePrivacy* s'affirment comme *lex specialis*, les unes par rapport à la directive 95/46/CE et l'autre par rapport au RGPD. On aurait tendance à en déduire qu'elles vont régir le traitement d'un certain type de données à caractère personnel, liées aux communications électroniques. Ce n'est pas aussi simple car cette règlementation s'inscrit également dans un paquet plus large de directives qui régissent la fourniture de services de communications électroniques.

Dans le cadre de cette règlementation, on retrouve principalement deux catégories des destinataires de règles : les fournisseurs de services et les abonnés/utilisateurs de ces services. Cela laisse donc présager que, lorsque l'on formule une condition ou restriction au traitement des données liées à une communication électronique, celui à qui cela s'adresse est le fournisseur de services. Autrement dit, la règlementation s'impose aux prestataires du secteur, mais pas à l'ensemble de la société. Cela impliquerait donc, en particulier, une protection qui n'existe que dans le cadre de la fourniture des services concernés par la règlementation.

Plaide en faveur d'une telle interprétation le fait que la directive 2002/58/CE ne porte que sur les réseaux qui sont utilisés entièrement

125 En vertu duquel « Les États membres peuvent adopter des mesures législatives visant à limiter la portée des droits et des obligations prévus aux articles 5 et 6, à l'article 8, paragraphes 1, 2, 3 et 4, et à l'article 9 de la présente directive lorsqu'une telle limitation constitue une mesure nécessaire, appropriée et proportionnée, au sein d'une société démocratique, pour sauvegarder la sécurité nationale – c'est-à-dire la sûreté de l'État – la défense et la sécurité publique, ou assurer la prévention, la recherche, la détection et la poursuite d'infractions pénales ou d'utilisations non autorisées du système de communications électroniques, comme le prévoit l'article 13, paragraphe 1, de la Directive 95/46/CE ».

ou principalement pour la fourniture de services de communications accessibles *au public*[126]. Le traitement de données à caractère personnel effectué dans le cadre de réseaux fermés ou privés d'une entreprise relève uniquement de la directive 95/46/CE et, depuis mai 2018, du RGPD. La directive ne couvre pas par exemple le traitement de données à caractère personnel dans le contexte d'un intranet d'une entreprise mais bien la communication de données via Internet[127–128]. On peut en induire que l'objectif premier de la législation n'est pas de consacrer un secret des communications électroniques, mais d'encadrer ce que les prestataires de services qui offrent des services accessibles au public peuvent ou non faire avec les données de communications et les communications générées par ce service.

De prime abord, il semble donc que l'objectif soit d'organiser le traitement des données dans le cadre des services prestés, et non le secret des communications lorsqu'elles ont lieu par des moyens électroniques. Le texte de la directive 2002/58/CE laissait toutefois une certaine marge aux États membres :

> « Les États membres garantissent, par la législation nationale, la confidentialité des communications effectuées au moyen d'un réseau public de communications et de services de communications électroniques accessibles au public, ainsi que la confidentialité des données relatives au trafic y afférentes. En particulier, ils interdisent à toute autre personne que les utilisateurs d'écouter, d'intercepter, de stocker les communications et les données relatives au trafic y afférentes, ou de les soumettre à tout autre moyen d'interception ou de surveillance, sans le consentement des utilisateurs concernés sauf lorsque cette personne y est légalement autorisée, conformément à l'article 15, paragraphe 1. Le présent paragraphe n'empêche pas le stockage technique nécessaire à l'acheminement d'une communication, sans préjudice du principe de confidentialité ».

Tel que formulé, le texte autorise à penser que l'interdiction peut être étendue à d'autres personnes que les fournisseurs de services.

L'exercice de la transposition en droit national permettait donc de donner une coloration plus ou moins étendue à ce principe d'interdiction

126 Art. 3 de la directive 2002/58/CE.

127 Y. POULLET, S. LOUVEAUX et M. V. PEREZ ASINARI, « Data Protection and Privacy in Global Networks : A European Approach », *The EDI Law Review*, 2001, p. 152.

128 Le Groupe de l'Article 29 a d'ailleurs regretté cette limitation du champ d'application en relevant que « les réseaux privés revêtent une importance croissante dans la vie de tous les jours et les communications des citoyens, par exemple dans le cadre de leur travail, et les risques que de tels réseaux font courir à la vie privée augmentent en conséquence et deviennent plus spécifiques (par exemple surveillance du comportement des salariés au moyen de données relatives au trafic, absence de confidentialité des communications) » (avis 7/2000 du 2 novembre 2000 sur la proposition, présentée par la Commission, de directive du Parlement européen et du Conseil concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques du 12 juillet 2000, COM(2000) 385, p. 3).

de poser les actes visés. En droit belge, par exemple, l'article 124 de la loi sur les communications électroniques du 13 juin 2005 qui transpose cette disposition a été interprété de longue date comme visant tout tiers non partie à la communication et pas uniquement les fournisseurs de service. Cela a une incidence sur l'impact de cette disposition dans le contexte des relations de travail. Ainsi, l'employeur non partie à la communication (par exemple un *e-mail* échangé entre un travailleur et un collègue ou une personne extérieure à l'organisation) est-il considéré comme un tiers qui se voit interdire notamment la prise de connaissance des communications s'il n'a pas l'autorisation de toutes les parties pour ce faire. Il s'agit donc d'une protection extrêmement forte qu'a choisi de consacrer le législateur belge.

46. L'adoption d'un règlement qui n'appelle plus de transposition au sein des États membres et qui pourrait conduire à l'abrogation de normes internes change la donne. Il est plus que jamais essentiel que le champ d'application *rationae personae* soit clair. Cela ne nous paraît pas être le cas dans la proposition de règlement *ePrivacy*.

L'article 5 de la proposition de règlement *ePrivacy* est libellé comme suit : « [l]es données de communications électroniques sont confidentielles. Toute interférence avec des données de communications électroniques, comme l'écoute, l'enregistrement, le stockage, la surveillance et d'autres types d'interception, de surveillance ou de traitement des données de communications électroniques, par des personnes autres que l'utilisateur final est interdite, sauf dans les cas où le présent règlement l'autorise ».

La façon dont le texte est rédigé peut laisser penser que la disposition est applicable à toute personne, quelle qu'elle soit, qui n'est pas partie à la communication, y compris un abonné (tel l'employeur) qui ne serait pas l'utilisateur final du service (tel le travailleur).

Il n'y a pas de disposition précisant qui sont les destinataires primaires de la proposition de règlement *ePrivacy*. Seul le huitième considérant de la proposition liste les personnes auxquelles le règlement est censé s'appliquer : « [l]e présent règlement devrait s'appliquer aux fournisseurs de services de communications électroniques, aux fournisseurs d'annuaires accessibles au public et aux fournisseurs de logiciels permettant des communications électroniques, y compris la récupération et la présentation d'informations sur Internet. Il devrait également s'appliquer aux personnes physiques et morales utilisant des services de communications électroniques pour envoyer des communications

commerciales de prospection directe ou recueillir des informations qui concernent l'équipement terminal de l'utilisateur final ou qui y sont stockées ».

Il faut donc constater que le texte de la proposition tel que libellé, ne semble pas inclure tout « tiers » à une communication dans le champ d'application du règlement. Aussi, la question de savoir si l'article 5 de la proposition de règlement *ePrivacy* pourrait être interprété comme faisant interdiction à un employeur de prendre connaissance par exemple d'un courrier électronique reçu par un travailleur reste-t-elle difficile à trancher vu ce qui précède. Le contrôleur européen à la protection des données a d'ailleurs appelé à une clarification et estime que « [l]e traitement des données de communications électroniques et des informations liées aux équipements terminaux des utilisateurs devrait relever, sans ambiguïté, du champ d'application du règlement "vie privée et communications électroniques", *quelle que soit l'entité chargée de traiter ces mêmes données*[129] »[130].

47. Une deuxième source d'incertitude provient du fait que le considérant 7 de la proposition de règlement *ePrivacy* laisse entendre, dans des termes quelque peu obscurs, que les États membres pourront adopter des dispositions nationales, sans expliciter concernant quels aspects du règlement ni avec quelle marge de manœuvre, en poursuivant l'objectif de « permettre de préserver un équilibre entre la protection de la vie privée et des données à caractère personnel et la libre circulation des données de communications électroniques ». Il n'est donc pas exclu que des dispositions de droit national soient maintenues ou adoptées, y compris concernant la question du secret des communications.

On rappellera encore que le RGPD permet aux États membres, en application de l'article 88, d'adopter des mesures spécifiques concernant le traitement des données dans les relations de travail.

Enfin, l'étendue de la protection suscite également le débat. En effet, le considérant 15 de la proposition de règlement *ePrivacy* laisse entendre que la protection liée au secret des communications ne prévaudra que *durant la transmission* de la communication et cesserait lorsque l'acheminement serait achevé. Cela fait l'objet de critiques de la part du

129 Souligné par l'auteur.

130 Contrôleur européen à la protection des donnée, avis 6/2017 sur la proposition de règlement relatif à la vie privée et aux communications électroniques (le règlement « vie privée et communications électroniques »), p. 20.

Groupe de l'Article 29 et du contrôleur européen à la protection des données[131]. Il n'est pas exclu que ce point soit revu : on conçoit mal qu'un élément aussi essentiel de la portée de la disposition ne soit précisé que dans un considérant.

Il résulte de ces éléments qu'il est difficile à l'heure actuelle de se faire une idée précise du régime qui prévaudra lors de l'adoption du règlement *ePrivacy*.

1. – *Les principales évolutions probables*

48. Le texte de la proposition publié le 10 janvier 2017 laisse toutefois présager de trois évolutions notables par rapport au régime actuel.

a) *Élargissement des réseaux concernés*

49. Comme évoqué ci-avant, la directive 2002/58/CE ne concerne que les communications effectuées au moyen d'un réseau public, à l'exclusion des réseaux privés.

Le futur règlement *ePrivacy* devrait englober plus généralement les services accessibles au public, indépendamment du fait que le réseau utilisé est un réseau public ou privé. L'objectif avoué est de toucher les services d'accès au wifi fournis par des entreprises commerciales à des clients de passage par exemple[132]. Cette modification a un impact limité concernant la problématique qui nous occupe dès lors qu'il est précisé que le règlement ne s'appliquera pas « aux groupes fermés d'utilisateurs finaux comme les réseaux d'entreprise dont l'accès est limité aux personnes faisant partie de la société »[133].

b) *Élargissement des supports de communications visés*

50. Il ne fait plus de doute que le marché des services de communication est en pleine évolution. Les services de *webmail*, de messagerie instantanée ou encore de « *Voice over IP* » proposés – souvent « gratuitement » – par des prestataires qui ne fournissent pas le service de base d'acheminement de la communication. Ces services remplacent aujourd'hui bien souvent d'autres modes de communications

131 Contrôleur européen à la protection des donnée, avis 6/2017 sur la proposition de règlement relatif à la vie privée et aux communications électroniques (le règlement « vie privée et communications électroniques »), p. 17 ; Groupe de l'Article 29, Opinion 01/2017 on the Proposed Regulation for the ePrivacy Regulation (2002/58/EC), WP 247, 4 avril 2017, p. 26.

132 Voy. considérant 13 de la proposition de règlement *ePrivacy*.

133 *Ibid*.

électroniques qui étaient l'apanage des fournisseurs de services de communications électroniques, tels que les opérateurs « télécoms » ou les fournisseurs d'accès à Internet. Le législateur européen affiche l'intention d'inclure ces fournisseurs de services via le Web dans la règlementation. Cela impliquerait, au niveau du secret des communications, que l'on ne ferait plus de différences entre un *e-mail* échangé entre deux employés et des messages échangés via Whats'app ou Messenger, ou un service de messagerie personnel lié à un réseau social, par exemple[134]. Le Groupe de l'Article 29 et le contrôleur européen estiment qu'il faudrait également viser expressément tous les messages échangés via de telles plateformes[135].

Cela pourrait concerner par exemple le mur d'un profil Facebook, ce qui laisse présager de riches débats. En effet, la jurisprudence rendue à ce sujet a plutôt eu tendance à se focaliser, pour conclure ou non à une protection, sur le caractère plus ou moins ouvert du support de diffusion du message. Le fait que les communications soient accessibles à un public indéterminé (par exemple, en raison du paramétrage du profil accessible à tout membre du réseau ou à un nombre indéfini de personnes) a conduit certains tribunaux, en France et en Belgique notamment, à considérer que les communications comme « non privées », et de ce fait non protégées[136].

c) *Élargissement des données concernées*

51. La proposition de règlement affiche clairement l'intention d'inclure, lorsqu'elle utilise le termes « données de communications électroniques »[137], à la fois le contenu de la communication[138] et les données générées par celle-ci pour les besoins de la transmission[139]. Elle étend ces communications électroniques protégées aux personnes morales. Il est précisé

134 Voy. considérants 1 et 11 de la proposition de règlement *ePrivacy*.

135 Contrôleur européen à la protection des données, avis 6/2017 sur la proposition de règlement relatif à la vie privée et aux communications électroniques (le règlement « vie privée et communications électroniques »), p. 31 ; Groupe de l'Article 29, Opinion 01/2017 on the Proposed Regulation for the ePrivacy Regulation (2002/58/EC), WP 247, 4 avril 2017, pp. 27 et 28.

136 S. CARNEROLI, *Les aspects juridiques des réseaux sociaux*, Bruxelles, Van den Broele, 2013, pp. 82-84.

137 Définies comme les « données de communications électroniques, le contenu de communications électroniques et les métadonnées de communications électroniques » (proposition de règlement *ePrivacy*, art. 4, k).

138 Définies comme « le contenu échangé au moyen de services de communications électroniques, notamment sous forme de texte, de voix, de documents vidéo, d'images et de son » (proposition de règlement *ePrivacy*, art. 4, l).

139 Définies comme les « les données traitées dans un réseau de communications électroniques aux fins de la transmission, la distribution ou l'échange de contenu de communications électroniques, y compris les données permettant de retracer une communication et d'en déterminer l'origine et la destination ainsi que les données relatives à la localisation de l'appareil produites dans le cadre de la fourniture de services de communications électroniques, et la date, l'heure, la durée et le type de communication » (proposition de règlement *ePrivacy*, art. 4, m).

dans le 3e considérant de la proposition de règlement que : « [l]es données de communications électroniques peuvent aussi révéler des informations concernant les personnes morales, telles que des secrets d'affaires ou d'autres informations sensibles ayant une valeur économique. Aussi les dispositions du présent règlement devraient-elles s'appliquer à la fois aux personnes physiques et aux personnes morales ».

Toutefois, derrière cette volonté d'extension de la protection, on constate qu'en réalité il ne s'agit pas de protéger les données des personnes morales. La protection octroyée a trait principalement à l'octroi de droits concernant l'insertion de données dans des annuaires, concernant l'utilisation de données aux fins d'envoi de communication non sollicitées[140]. Lorsque l'on parle de protection des communications électroniques (un *e-mail*, par exemple) en tant que telles, la personne protégée est l'utilisateur final, à savoir une personne physique qui utilise le service de communications électroniques (par exemple, le service de messagerie)[141-142].

C. – *Conclusion*

52. Les contours de la protection peuvent recouvrir des cas de figure tout à fait variables selon que l'on inclut ou non tout tiers comme destinataire de la norme et que l'on vise plus ou moins largement les communications électroniques concernées. L'incidence de telles modifications pourrait potentiellement être conséquente dans le contexte d'un contrôle des communications des travailleurs mais cette incidence reste incertaine.

V. La réponse du droit européen est-elle à la hauteur du défi ?

53. Le moins que l'on puisse dire, c'est que les textes évoqués laissent une certaine souplesse pour répondre à la problématique et aux difficultés soulignées en guise d'introduction générale. C'est sans doute

140 Voy. ch. III de la proposition de règlement *ePrivacy*.

141 Voy. not. les art. 5 et 12 de la proposition de règlement *ePrivacy*.

142 Le Groupe 29 appelle d'ailleurs à un assouplissement des règles relatives au consentement de l'utilisateur final lorsqu'il s'agit d'interférer avec des données associées à un outil mis à disposition d'un travailleur par l'employeur et que cette interférence est nécessaire pour assurer le bon fonctionnement de cet outil. Groupe de l'Article 29, Opinion 01/2017 on the Proposed Regulation for the ePrivacy Regulation (2002/58/EC), WP 247, 4 avril 2017, p. 29 ; Groupe de l'Article 29, Opinion 2/2017 on Data Processing at Work, WP 249, 8 juin 2017, p. 5.

qu'il n'y a pas une bonne solution, mais plutôt des bonnes pratiques à développer pour accompagner le développement de l'usage des technologies de communications dans le monde du travail. Il est évident qu'il s'agit d'un phénomène en mutation constante et qu'il faudra adapter, ajuster et évoluer avec les usages propres à l'entreprise ou à l'autorité publique agissant en qualité d'employeur.

Il nous semble contreproductif de vouloir consacrer un secret absolu des communications électroniques dans le contexte des relations de travail dès lors que cela méconnaît les réalités de la vie de l'entreprise ou de l'autorité publique. Il serait également hypocrite de reconnaître un droit au respect de la vie privée au travail, incluant le droit de communiquer sur ce lieu du travail et de le réduire à néant en permettant de considérer que toutes les communications échangées via le réseau de l'employeur sont professionnelles pour y greffer un droit de contrôle absolu. Le bon arbitrage se trouve entre les deux extrêmes. Permettre un usage et un contrôle des écrits électroniques, mais dans un cadre balisé qui ménage les droits et prérogatives de l'employeur et du travailleur.