Elena LAZĂR[*]

La jurisprudence CEDH post Bărbulescu dans le contexte de surveillance des employées – évolution et conséquences

I. Introduction

La question du droit pour un employeur d'effectuer une surveillance de ses employés au travail et hors du travail n'est pas du tout nouvelle, prenant en compte l'arrivée de nouvelles technologies, mais il n'existe toujours pas de réponse définitive portant sur cet aspect-là. Le droit de surveillance d'un employeur sur le lieu de travail est souvent méconnu par les salariés. Internet, téléphone, badges d'accès, caméras etc., tous ces moyens permettent de surveiller et contrôler l'activité des employées. Mais sont-ils tous licites au regard du droit du travail et du respect de la vie privée?

Il est donc important de souligner dans ce contexte que les relations de travail, en tant que rapport juridique et bien créditées parfois d'une certaine confiance, n'échappent pas toutefois à des abus.

Un employeur a toujours la possibilité d'accéder à l'ordinateur mis à la disposition de son salarié dans le cadre de son travail. Mais peut-il librement consulter les fichiers, les connections ou les emails qui y figurent, surtout quand le salarié est absent?

En principe, l'accès à internet au travail doit servir comme outil seulement pour l'exécution des taches professionnelles et ne pas être utilisé à des buts personnels par le salarié, mais en pratique, son utilisation à des fins privées arrive d'être souvent tolérée dès lors qu'elle n'est pas abusive. Quand même ça peut générer des problèmes parce qu'en fait l'employeur peut contrôler les connexions Internet du salarié même en son absence, puisque celles-ci sont présumées avoir un caractère professionnel.

Aussi l'employeur a la possibilité d'accéder les fichiers figurant sur le disque dur de l'ordinateur de son salarié, hormis lorsque son employé a identifié ces documents comme étant personnels.

Beaucoup de salariés ont librement accès au téléphone dans le cadre de leur travail. Cette liberté peut parfois conduire à des abus lorsque le salarié utilise la ligne téléphonique de son entreprise pour passer de longs appels sans aucun lien avec l'exécution de son travail. D'autres moyens de contrôle assez souvent utilisés par les grandes entreprises de nos jours sont les badges électroniques permettant de vérifier les horaires d'entrée et de sortie du salarié dans l'entreprise en vue de contrôler l'activité ou même des dispositifs de surveillance vidéo.

Vis- à vis de tous ces aspects il faut s'interroger qu'elle a été la position de la Cour Européenne des droits de l'homme (la Cour) après son jugement dans l'affaire Bărbulescu, tout en prenant en compte l'imminence de RGPD**.**

---

[*] *Teaching assistant at the Law Faculty, University of Bucharest*
E-mail: lazar_elena2@yahoo.com
Manuscris primit la 18 martie 2018

II. Les principes développés par la jurisprudence Bărbulescu

Quelques mois seulement avant la mise en application du Règlement Général Européen sur la Protection des Données (RGPD), la Cour a rendu le célèbre arrêt selon lequel une entreprise qui surveillait la correspondance privée de ses salariés violait le droit au respect de la vie privée de ceux-ci. Quel est l'impact de cette affaire sur la façon dont les entreprises devront se mettre en conformité avec le RGPD?

En effet, les communications privées entrent dans la définition des données personnelles fournie par l'article 4 du RGPD[1], qui dispose que l'entreprise doit prouver qu'elle a des raisons légitimes de collecter et surveiller les données de ses salaries.

On apprécie donc qu'il s'avère important de souligner qu'étant donné le déséquilibre existent de la relation entre un employeur et un salarié, le consentement de ce second n'est pas en fait effectif, parce qu'en cas de refus, il risque de se mettre dans une situation délicate en refusant d'être surveillé. Donc, dans ce cas, dans les rapports salaries-employeurs, les entreprises devront donc simplement se trouver dans l'une des situations légitimes de traiter les données, exposées par RGPD, et non pas se baser sur le consentement des employées[2]. L'employeur pourra faire valoir son intérêt légitime par exemple dans le contexte du contrôle du travail de l'employé, mais en aucun situation, il pourra se prévaloir de procédures extensives et automatisées ou se servir de méthodes qui ne permettent aucun contrôle a posteriori, comme par exemple contrôler l'historique internet du salarié à son poste de travail.

Dans l'affaire Bărbulescu[3], rendu le 5 septembre 2017, sur renvoi de l'affaire (après que la chambre saisie ait abouti, le 12 janvier 2016, à un constat de non violation de l'article 8 de la Convention) la Cour avait considéré que les juridictions roumaines avaient méconnu les dispositions de l'article 8 de la Convention européenne de sauvegarde des libertés fondamentales et des droits de l'Homme («la Convention») en validant le licenciement d'un salarié qui avait utilisé à des fins personnelles sa messagerie professionnelle, en violation du règlement intérieur de l'entreprise. En effet, elle a souligné dans son arrêt que le dispositif de surveillance mis en place par l'employeur et la sanction infligée au salarié n'étaient pas conformes aux principes de transparence, de finalité et de proportionnalités requises par l'article 8 de la Convention.

On entend d'évoquer la jurisprudence Bărbulescu car on apprécie qu'il s'agisse d'un message fort qu'a adressé la Cour aux compagnies privées, pour ce qui est de la surveillance qu'elles exercent sur la correspondance électronique de leurs employées.

Monsieur Bărbulescu, ressortissant roumain, employé par une entreprise privée du 1ier août 2004 au 6 août 2007 comme ingénieur en charge des ventes, poste pour lequel il ouvrit un compte Yahoo Messenger, afin de communiquer avec ses clients. En juillet 2007, l'entreprise vient d'informer son personnel par note interne qu'un salarie venait d'être licenciée pour motif disciplinaire, pour avoir utilisé internet, téléphone et photocopieur à des fins personnelles. Le 13 juillet 2007, M. Bărbulescu, convoqué par son employeur, apprit que ses communications sur Yahoo Messenger avaient été surveillées et qu'il était donc soupçonné

[1] (*http://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:32016R0679&from=FR*) consulté le 18 mars 2018.

[2] *D.N. Costescu*, Regimul juridic european al prelucrării datelor cu caracter personal, Thèse doctorale soutenu en septembre 2015, coordonnateur Corneliu Liviu Popescu, p. 302.

[3] CEDH, *Bărbulescu c. Roumanie*, req. n° 61496/08, 5 Septembre 2017.

d'utiliser internet à des fins personnelles. Comme il n'a pas reconnu les allégations, l'employeur lui fournit la transcription de 45 pages de ses communications, entre le 5 et le 12 juillet, révélant les échanges privés, intimes, avec sa fiancée et son frère. Par conséquent, le requérant fut licencié, le 1ier août 2007, pour ne pas avoir respecté le règlement intérieur de l'entreprise, qui interdisait donc l'usage à des fins privées des ressources de celle-ci.

Bărbulescu porta l'affaire devant les tribunaux roumains, pour atteinte à son droit à la correspondance, la violation des dispositions de la Constitution et du code pénal entachant, selon lui, de nullité la procédure de licenciement. Toutefois, tant le tribunal de Bucarest que la Cour d'appel ont rejeté son recours, estimant que l'entreprise était en droit de fixer des règles quant à l'utilisation d'internet, et que le requérant avait été dûment informé du règlement intérieur de l'entreprise.

La Cour, saisie en 2008, a estimé dans son arrêt de chambre du 12 janvier 2016 (par six voix contre une-position qui s'avérer assez étonnante), que les juridictions internes avaient ménagé «un juste équilibre» entre le droit du requérant au respect de sa vie privée et les intérêts de son employeur. L'arrêt vient d'être cassé par la Cour en grande chambre, la conclusion étant celle d'une violation de l'article 8 de la Convention, cette fois les juges estimant que les juridictions internes n'ont pas réussi a ménager le juste équilibre entre les intérêts en jeu, résultat qui représente bien on dirait un renforcement des droits des salariés en la matière.

La Cour souligne plus particulièrement l'idée selon laquelle la vie privée au sens de l'article 8 inclut «le droit de mener une „vie privée sociale", à savoir la possibilité pour l'individu de développer son identité sociale»[4]. En plus, les juges rajoutent qu'en ce qui concerne les activités professionnelles, que «les 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»[5], affirmation qui laisse de la place pour l'interprétation.

La Cour rappelle ensuite que, selon sa jurisprudence constante, les communications émanant de locaux professionnels se trouvent comprises dans les notions de «vie privée» et de «correspondance» visées à l'article 8. Ceci lui permet de constater sans difficulté que la messagerie instantanée sur internet employée par le requérant (Yahoo Messenger) est évidemment une «forme de communication faisant partie de l'exercice d'une vie privée sociale» (§74).

Le problème donc qui s'est posée ici est si tandis que nul ne conteste que l'usage d'une messagerie instantanée sur internet comme Yahoo Messenger fait partie intégrante de la vie sociale d'un individu, il reste à trancher si une telle activité *personnelle* est permise sur le lieu de travail et si oui, dans quelles conditions.

Un point clé de l'analyse de la Cour consiste ici, non seulement dans le fait que le salarié n'était en réalité pas clairement informé du fait que ses communications aient été surveillées, mais non plus même qu'une surveillance pouvait être effectuée à son encontre.

La juridiction européenne estime ainsi au total que «les instructions d'un employeur ne peuvent pas réduire à néant l'exercice de la vie privée sociale d'un individu [et que] le respect de la vie privée et de la confidentialité des communications continue à s'imposer, même si ces

[4] CEDH, *Bărbulescu c. Roumanie*, req. n° 61496/08, 5 septembre 2017, §70.
[5] Idem, §71.

dernières peuvent être limitées dans la mesure du nécessaire»[6]. Il résulte donc que l'article 8 est donc applicable en l'espèce.

Si la solution ne nous surprend pas, il résulte clairement que la Cour dessine ici les contours d'un statut très protecteur du salarié s'agissant du respect de sa vie privée dans le cadre d'une entreprise. La Cour vient donc de relever en effet les obligations positives de l'Etat d'assurer aux personnes la garantie de la jouissance d'un droit consacré par la Convention (article 8). Ainsi le raisonnement de la Cour a été donc de vérifier si un «juste équilibre» a été ménagé entre l'intérêt général et les intérêts de l'individu, ce qui correspond à son très classique contrôle de la proportionnalité, qui doit être nécessairement pondéré par l'existence de la «marge d'appréciation» dont disposent les Etats.

Pratiquement la Cour a essayé de répondre à suivantes questions à travers son arrêt: L'employeur va-t-il avancer des motifs légitimes pour justifier la surveillance de ces communications et l'accès à leur contenu même? Aurait-il été possible de mettre en place un système de surveillance reposant sur des mesures moins intrusives que l'accès direct au contenu des communications de l'employé? Quelles ont été les conséquences de la surveillance pour l'employé qui en a fait l'objet? De quelle manière l'employeur va-t-il utiliser les résultats de la mesure de surveillance, et, notamment, ces résultats ont-ils été utilisés pour atteindre le but déclaré de la mesure?

On entend souligner ici que le litige, à la base, se situe dans le cadre d'une relation contractuelle (employeur-salarié), sachant que des mesures protectrices *peuvent* être prévues par le droit du travail, l'employeur disposant de prérogatives certaines dans l'organisation du travail: il a le pouvoir de direction et à ce titre, il peut contrôler, surveiller et sanctionner l'activité des salariés pendant leur temps de travail[7]. L'employeur peut même mettre en place des outils de contrôle individuel pour sécuriser l'accès des bâtiments comme des badges ou même la circulation dans les locaux. Ces outils peuvent également être utilisés pour gérer les horaires de travail, comme par exemple des programmes informatique ou les salaries vont introduire les temps travaille pour chaque projet. Toutefois la surveillance mise en place doit être justifiée par la tâche et proportionnée au but envisage.

C'est donc la raison pour laquelle la Cour va s'attacher dans cet arrêt à apprécier le juste équilibre entre les différents intérêts en jeu. Elle reconnaît tout d'abord que le requérant était informé du règlement intérieur, prohibant l'usage des ressources de l'entreprise à des fins personnelles, mais exprime son soucie quant à l'information de l'intéressé au sujet de la surveillance mise en œuvre à son encontre, aussi bien dans sa nature que dans son étendue. La juridiction européenne reproche ainsi aux juridictions nationales, le fait de n'avoir pas recherché si monsieur Bărbulescu avait été averti de façon préalable de la possibilité d'une surveillance par l'employeur, ainsi que de la nature et de l'étendue de cette dernière. Un autre reproche est celui de n'avoir pas vérifié «la question de savoir si le but poursuivi par l'employeur aurait pu être atteint par des méthodes moins intrusives»[8].

Le constat de violation de l'article 8 opéré par la Cour vient d'encadrer d'une façon très stricte les mesures de surveillance de la correspondance électronique de leurs salariés, que les compagnies/employeurs seraient tentées peut être de mettre en œuvre. Elle impose donc

[6] Idem, §81.

[7] Article 29 Data Protection working Party, *Guidelines on Consent under Regulation 2016/679*, 28 novembre 2017.

[8] CEDH, *Bărbulescu c. Roumanie*, req. n° 61496/08, 5 septembre 2017, §136.

quatre conditions fondamentales à respecter en la matière: une information préalable des salariés, une information précisant la nature et l'étendue de la surveillance effectuée, la détermination de raisons qui justifient la mise en place de mesures de surveillance, et finalement le fait que soit envisagée par l'employeur la possibilité de prendre de mesures moins intrusives pour la vie privée des requérants.

On apprécie que les principes/conditions tirés par la Cour du présent arrêt représentent un progrès remarquable pour les droits des salariés.

Toutefois, la vidéosurveillance représente une pratique faisant encore l'objet de plusieurs débats. Comment protéger sa vie privée et ses données personnelles dans le cadre d'une vidéosurveillance? C'est la question à laquelle la juridiction européenne doit répondre dans les affaires suivant la jurisprudence Bărbulescu, Ribalda[9] *et Antovic*[10]*. Ces affaires relancent, une fois de plus, le débat à propos de la vidéosurveillance et leurs effets sur les salaries.*

III. La vidéosurveillance des salaries: une question épineuse portée de nouveau devant la CEDH- les implications de la jurisprudence qui suit l'affaire Bărbulescu

Dans deux affaires, la juridiction européenne a fallu se prononcer si la mise en place de vidéosurveillance dans certains lieux portait ou non atteinte à la vie privée.

L'affaire *Antović et Mirković c. Montenegro*, rendue par la Cour européenne en novembre 2017, nous amène devant la situation de deux ressortissants du Monténégro, professeurs d'une université de mathématique. Invoquant comme raison la protection des personnes, de la propriété et la surveillance de l'enseignement, le doyen de la faculté a décidé par conséquent d'installer des caméras de vidéosurveillance dans les amphithéâtres. Les membres de l'université ont été par suite informés de la mise en place de ce dispositif. Les deux requérants, les enseignants Mme Antović et M. Mirković se sont alors plaints auprès de l'Agence de protection des données personnelles en s'opposant à la mise en place d'un tel dispositif en précisant qu'il existait d'autres systèmes moins intrusives ayant comme but de contrôler la protection des personnes et de la propriété. Le conseil de l'Agence considéra qu'il n'existait aucune raison valable pour mettre en place telle vidéosurveillance car il n'y avait pas de danger apparent pour les personnes ou pour leur propriété. De plus, la mesure de surveillance n'était pas conforme à la protection des données personnelles selon le conseil. Les caméras furent donc retirées. Toutefois les professeurs demandèrent réparation en justice sur le fondement de l'article 8 de la Convention qui protège la vie privée, mais les tribunaux nationaux ont décidé de rejeter cette demande au motif que la question de la vie privée ne se posait pas en l'espèce car les amphithéâtres où Mme Antović et M. Mirković enseignaient étaient des lieux publics et que les données récoltées sur les caméras ne représentent pas des données personnelles.

Ainsi, l'affaire est portée devant la Cour. La juridiction européenne souligne que la notion de vie privée existe bien même s'il s'agit du lieu de travail comme elle l'a déjà fait antérieurement dans sa jurisprudence, la vie privée pouvant donc inclure les activités professionnelles. Dans le présent cas, il résulte clairement que les amphithéâtres sont les lieux de travail des enseignants, tout en relevant à ce titre que les professeurs d'université n'ont pas

[9] CEDH, *López Ribalda et autres c. Espagne*, req. n°1874/13, 9 janvier 2018.
[10] CEDH, *Antović et Mirković c. Montenegro*, req. n°70838/13, 28 novembre 2017.

seulement une fonction d'enseignement, mais ils créent aussi une véritable relation avec leurs étudiants en interagissant avec eux[11].

Ainsi, les juges de la Cour européenne ont entendu invoquer la jurisprudence antérieure, Bărbulescu[12], à laquelle on a déjà fait référence, ou il a été jugé que la vidéosurveillance secrète au travail constituait une intrusion dans la vie privée des salariés. Elle décide d'appliquer cette décision même si les salariés ont été avertis de la mise en place du tel dispositif. La Cour en conclu qu'il existe une ingérence dans les droits des salariés du fait de la mise en œuvre de la vidéosurveillance des employées de la faculté et qu'il y a eu donc violation de l'article 8 de la Convention, estimant dans ce cas qu'une simple précaution de la potentielle protection des salariés et de la propriété ne justifie en aucun situation la mise en place d'une telle mesure.

Une autre affaire portant aussi sur le même sujet de la vidéosurveillance, *Lopez Ribalda c. Espagne* rendu le 9 janvier 2018 concerne un cas de vidéosurveillance dissimulée cette fois, sur un lieu de travail. Les requérantes, Isabel López Ribalda, María Ángeles Gancedo Giménez, María Del Carmen Ramos Busquets, Pilar Saborido Apresa et Carmen Isabel Pozo Barroso sont cinq ressortissantes espagnoles qui résident à Sant Celoni et Sant Pere de Vilamajor, en Espagne et qui occupaient toutes un emploi de caissière chez M.S.A, représentant une chaîne de supermarché familiale. Après avoir constaté une disparité entre les stocks et les chiffres de ventes quotidiennes, l'employeur a pris la décision de mettre en place un système de vidéosurveillance dans le marché et pour mettre en œuvre son dispositif, il a installé certaines caméras visibles mais aussi des caméras cachées. Les salariées ont été par conséquent informées de la mise en place d'un tel dispositif, mais seulement sur les cameras qui étaient visibles, et non pas sur les caméras cachées. Les faits de vols des salariés se répétèrent alors et ils ont été convoqués à des entretiens lors desquels une vidéo de leurs faits leur a été montrée, entrevue suivi bien sûr par un licenciement disciplinaire.

Suite à ces licenciement les requérantes ont saisi la juridiction du travail. D'une façon prévisible on pourrait dire, la décision rendue en première instance a confirmé la décision de l'employeur du magasin, mais aussi décision d'appel s'est ralliée aussi à l'avis des juges de première instance. Il fut admis que les enregistrements pris par les caméras de vidéosurveillance cachés étaient des preuves acceptables car obtenues de manière légale. Afin de justifier le fait que l'employeur n'a pas informé ses salariées sur l'existence de certaines caméras placées dans le magasin, les juridictions nationales ont admis l'existence de soupçons raisonnables de vol. Elles ont estimé que la mise en place d'un tel dispositif de vidéosurveillance représentait pratiquement la seule possibilité pour l'employeur, de voir protégés ses intérêts.

Vue les décisions des juridictions nationales, la Cour européenne qui a été saisi, a dû répondre à la question de savoir si le dispositif mis en œuvre par l'employeur était licite ou pas et si la mise en balance des intérêts a été correcte, aspect qui pose de nouveau la question de la proportionnalité de la mesure prise[13].

---

[11] Ibidem.

[12] CEDH, *Bărbulescu c. Roumanie*, req. n° 61496/08, 5 septembre 2017.

[13] Concernant la subsidiarité du contrôle opéré par la Cour de Strasbourg, voir *C.G. Achimescu*, Principiul subsidiarității în domeniul protecției europeane a drepturilor omului (Le principe de susidiarité dans la protection européenne des droits de l'homme), Ed. C.H. Beck, Bucarest, 2015, p. 176, p. 98.

Comme on a déjà précisé dans notre démarche, pour mettre en place un tel dispositif une balance doit être faite entre les intérêts de l'employeur et la sauvegarde de la vie privée des salariés. Selon la juridiction européenne, la mesure mise en œuvre dans la présente affaire ne respectait pas ce principe de proportionnalité, vu qu'il aurait été possible de protéger les droits de l'employeur sans recourir à de tels moyens intrusifs. En plus les salariées n'avaient pas été informées de l'étendue du dispositif mis en œuvre. La Cour a donc conclu que les juridictions nationales n'ont donc pas ménagé un juste équilibre entre le droit des requérantes au respect de leur vie privée et les droits patrimoniaux de l'employeur.

La décision nous semble assez surprenante pour les employeurs en ce que les délits de vol des salariées ont été avérés grâce à la mise en place de ce système de surveillance, mais en dépit de ça, apparemment quand il 's'agit des relations de travail et la protection des données personnelles, c'est l'intérêt prive qui prime, et pas celui de l'employeur.

Si dans l'affaire Bărbulescu la décision et implicitement la ligne d'argumentation, ne nous a pas paru très surprenante, prenante en compte les circonstances de fait, la solution envisagée par la Cour dans l'affaire Ribalda, vue qu'il s'agit quand même d'une infraction, s'avère toutefois étonnante. En effet, on apprécie que l'aspect qui a gagné le plus des poids ait été celui du caractère caché des caméras, aspect qui a guidé la solution de la Cour. En rendant une telle décision la juridiction européenne a clairement mis un frein dur à la mise en place de la vidéosurveillance de ses salariés

Toute cette jurisprudence qu'on a évoquée vient de montrer la place de la Cour européenne qui apparemment vient de prohiber grandement ce genre de dispositifs de vidéosurveillance au lieu de travail.

Quand même on ne peut pas ne rappeler une affaire antérieure et assez similaire de la juridiction européenne ou elle a toutefois accepté la mise en œuvre d'une vidéosurveillance par les employeurs, dans des circonstances semblables à l'affaire Ribalda. On fait ici référence à l'affaire *Köpke c. Allemagne*[14] du 5 octobre 2010 dans laquelle une salariée fut licenciée pour vol à la suite de la découverte par son employeur grâce à un dispositif pareil de vidéosurveillance secrète. Même si, il s'agissait aussi d'une caméra secrète, la Cour a jugé que l'employeur avait bien respecte le test de proportionnalité entre la vie privée de la salariée et les intérêts de l'employeur avant de mettre en place la surveillance, en soulignant que la surveillance par vidéo a été délimitée dans le temps et l'espace et par conséquent, grâce à ces éléments, elle en a déduit qu'il n'y avait pas eu d'atteinte à la vie privée de la requérante: «La Cour relève en outre que les juridictions internes étaient conscientes que la mesure de surveillance était limitée dans le temps – elle a été appliquée pendant deux semaines. Ils avaient également pris note du fait que la mesure était limitée à l'égard de la zone qu'elle couvrait en ce qu'elle ne s'étendait pas au lieu de travail du requérant dans le supermarché et le département des boissons dans son ensemble, mais couvrait seulement la zone située derrière et incluant La caisse, le caissier et la zone entourant immédiatement la caisse, qui, de plus, ne pouvaient pas être considérés comme un endroit particulièrement isolé puisque le service des boissons en tant que tel était accessible au public»[15].

Cette décision prouve bien encore une fois que le plus important est le test de proportionnalité que l'employeur doit effectuer et donc toute mesure qui pourrait venir

[14] CEDH, *Köpke c.Allemagne*, req. n° 420/07, 5 octobre 2010.
[15] Ibidem.

entraver le droit à la vie privée et intime des salariés doit être justifiée par des motifs légitimes et importants et seulement une simple mesure de précaution ne suffit pas.

Toutefois, faisant une comparaison avec l'affaire Ribalda évoquée ci-dessus, ce qui apparaît étonnant c'est que même face un acte illégal de la part des employées, la Cour protège tout de même leur vie privée par rapport aux intérêts de l'employeur. Il faut se poser donc, dans ces conditions la question de savoir dans quelles circonstances une vidéosurveillance pourra être mise en place notamment sur un lieu de travail.

En plus, une autre différence entre les deux affaire, dont la juridiction européenne a probablement tenu compte, réside dans le fait que dans l'affaire Ribalda, la législation en vigueur clairement établissait que chaque collecteur de données devait informer les personnes concernées de l'existence de moyens de collecte et de traitement de leurs données personnelles et donc si le droit de chaque personne concernée d'être informé de l'existence, étendue et les modalités de la surveillance vidéo cachée a été clairement réglementé et protégé par la loi, les requérants jouissent d'une attente raisonnable en ce qui concerne la protection de la vie privée. De plus, dans ce cas, et contrairement à l'affaire Köpke, la surveillance vidéo cachée ne constituait pas une conséquence d'une suspicion antérieure avérée contre les requérants et par conséquent, ils ne se réfèrent pas spécifiquement à eux, mais à tout le personnel travaillant dans les caisses enregistreuses, pendant plusieurs semaines, sans limite de temps et pendant toutes les heures de travail. Comme on a déjà précisé, dans l'affaire Köpke, la surveillance était limitée dans le temps – elle durait deux semaines – et seulement deux employés étaient concernés. Cependant, dans l'affaire Ribalda, la décision d'entreprendre des mesures de surveillance reposait sur une suspicion générale à l'encontre de tout le personnel, compte tenu des irrégularités précédemment constatées par le gérant du magasin.

Comme une conclusion qui ressort de ces affaires c'est que l'employeur souhaitant mettre en œuvre un dispositif de surveillance vidéo doit au préalable effectuer un test de proportionnalité avec une grande attention et soucie afin de ne pas porter atteinte aux droits et libertés de ses salariés.

Toutefois, on pourrait considérer le jugement de la Cour dans l'affaire Ribalda comme un revirement de jurisprudence, par rapport à l'affaire Köpke, revirement prévisible si on prend en compte la phrase même de la juridiction européenne dans cette décision: «La Cour observe cependant que l'équilibre établi entre les intérêts en cause par les autorités internes ne semble pas être le seul moyen possible pour eux de s'acquitter des obligations qui leur incombent en vertu de la Convention. Il se peut fort bien que les intérêts concurrents en cause aient un poids différent à l'avenir, compte tenu de la mesure dans laquelle les intrusions dans la vie privée sont rendues possibles par de nouvelles technologies de plus en plus sophistiquées»[16].

IV. L'affaire *Libert c. France* - involution jurisprudentielle ou attitude réservée de la Cour?

Un ex-salarié de la SNCF[17] qui a vu son dossier informatique „personnel" fouillé en son absence, sans information préalable, et dont le contenu a été retenu contre lui pour motiver un licenciement vient de se voir refuser, la reconnaissance d'une violation de son droit au respect de la vie privée

[16] Ibidem.

[17] CEDH, *Affaire Libert c. France*, n°588/13, 22 fevrier 2018.

Pour rejeter la demande, les juridictions internes se sont appuyées sur la possibilité reconnue à l'employeur d'accéder aux fichiers non identifiés comme prives. Dans la présente affaire, la SNCF a fait valoir qu'elle avait prescrit, via une charte informatique de l'utilisateur, d'utiliser le terme „privé" pour identifier les informations à caractère strictement personnel. De plus, les juges ont retenu que les documents consultés se trouvaient dans un dossier servant *„traditionnellement"* aux agents à stocker leurs documents professionnels.

Cette solution s'avère aussi très surprenante, vue que la CEDH dans l'affaire Bărbulescu antérieurement analysée, a jugé en Grande Chambre, après l'utilisation du test de proportionnalité, que l'employeur avait violé le droit à la vie privée et familiale, tout en déclarant illégal le système de surveillance utilisé pour aménager la preuve de la faute du salarié.

Comme on peut déduire de la présente affaire, la juridiction européenne n'a pas tenu compte de ces quatre critères poses dans la jurisprudence Bărbulescu, que nous avons évoqué au début de notre démarche, ce qui nous amène à la question de savoir quel a était son raisonnement, qu'est-ce que distinguent les deux affaires.

Premièrement, l'affaire porte sur des correspondances privées, tandis que la présente affaire porte sur la consultation des fichiers. Ce qui nous amène a une deuxième question: Consulter des fichiers et consulter des correspondances s'avèrent vraiment des modalités d'ingérence dans la vie privé des employées si éloignées l'une de l'autre? Deuxièmement, le jugement du 5 septembre 2017 implique un employeur de droit privé alors que celui du 22 février 2018 concerne une autorité publique, tandis que le contrat de travail était de droit privé.

Une autre hypothèse serait d'admettre que les juges ont aussi tenu compte de la nature des faits constatés. Les faits et le contexte étaient toutefois substantiellement différents. En effet, dans l'affaire Bărbulescu, les faits retenus comportaient 45 pages de transcription de communications entretenues avec le frère et la fiancée du salarié dont le contenu n'a pas été divulgué. Tandis que, dans la présente affaire, un cadre de la SNCF a été suspendu de ses fonctions à la suite d'une mise en examen pour dénonciation calomnieuse, mais comme un non-lieu est prononcé, l'intéressé a demandé d'être réintégré dans ses anciennes fonctions. A son retour il constate que son ordinateur a fait l'objet d'une saisie et que l'employée qui lui avait remplacée avait trouvé sur son disque dur des attestations de résidence de complaisance destinées à des tiers et des fichiers à caractère pornographique, plus précisément, 562 fichiers à caractère pornographique, dont certains à caractère zoophile ou scatophile, représentant un volume total de 787 mégaoctets, ce qu'il a signalé à sa hiérarchie.

L'agent est licencié aux motifs que tous ces faits sont contraires à l'obligation d'exemplarité particulière liée à ses fonctions et aux dispositions de normes internes, notamment la charte des systèmes d'information. Par conséquent, dans cet arrêt la Cour, tout en considérant que la SNCF, autorité publique, s'était ingérée dans le droit au respect de la vie privée d'un agent licencié, a conclu que l'ingérence poursuivait un but légitime et qu'elle constituait, en l'espèce, une mesure nécessaire dans une société démocratique.

Au terme de la procédure contentieuse qu'engage l'agent licencié, la Cour de cassation, par un arrêt du 4 juillet 2012, donne raison aux juges du fond d'avoir reconnu le bien-fondé de son licenciement, estimant que cet usage abusif et contraire aux règles en vigueur au sein de la SNCF. Invoquant l'article 8 de la Convention, l'agent s'est plaint devant la Cour d'une violation de son droit au respect de sa vie privée résultant du fait que son employeur avait ouvert, hors de sa présence, des fichiers figurant sur le disque dur de son ordinateur professionnel sous un intitulé *«données personnelles»*.

La première question était de savoir si la SNCF pouvait être regardée comme une «autorité publique» au sens de l'article 8 de la Convention et s'il peut y avoir d'ingérence d'une autorité publique dans l'exercice du droit au respect de la vie privée que pour autant que cette ingérence soit prévue par la loi et qu'elle constitue une mesure qui, dans une société démocratique, est notamment nécessaire à la prévention des infractions pénales ou encore à la protection des droits et libertés d'autrui. Le Gouvernement français contestait l'applicabilité de l'article 8 de la Convention au motif que la SNCF est un établissement public industriel et commercial, que son personnel relève du droit privé, que les décisions non réglementaires qui régissent le personnel en question sont des actes de droit privé et qu'enfin les litiges le concernant relèvent du juge judiciaire.

La Cour n'a pas retenu les arguments de Gouvernement français, estimant que la SNCF était bien une personne morale de droit public, placée sous la tutelle de l'Etat et donc il convenait en conséquence d'analyser les griefs du requérant sous l'angle des obligations négatives de l'Etat.

D'une part, selon la Cour, l'ingérence de la SNCF était prévue par la loi vue le contenu des articles L 1121-1 et L 1321-3 du Code du travail[18] indiquent qu'au sein de l'entreprise nul ne peut apporter aux droits des personnes et aux libertés individuelles et collectives des restrictions qui ne seraient pas justifiées par la nature de la tâche à accomplir ni proportionnée au but recherché et que le règlement intérieur établi par l'employeur doit respecter les mêmes limites. D'autre parte, l'ingérence était par ailleurs justifiée et poursuivait un but légitime dans une société démocratique.

Même si le gouvernement français soutenait que le but légitime était représenté par la prévention des infractions pénales, la cour ne retient pas cet argument, mais précise que l'employeur avait un intérêt légitime d'assurer le bon fonctionnement de l'entreprise pour que ses salariés utilisent les équipements informatiques mis à leur disposition en conformité avec leurs obligations contractuelles et la réglementation applicable. Donc il résulte d'une manière très claire du raisonnement de la Cour qu'en poursuivant un but légitime, l'employeur est en mesure d'ouvrir les fichiers professionnels qui se trouvent sur le disque dur des ordinateurs professionnels de ses salariés et statue par conséquent qu'il n'y a pas eu violation de l'article 8 de la Convention. Mais qu'est qu'il en reste quand il s'agit des fichiers dénommés personnels comme le cas dans notre espèce?

La Cour justifie cette solution par le fait que d'une part la Charte d'utilisateur pour l'usage du système d'information de la SNCF indiquait expressément que les informations à caractère privé devaient être dénommes avec le terme «privé» et non avec le terme «personnels» et d'autre part le salarie avait utilisé une partie très importante du hard de son ordinateur professionnel pour stocker les fichiers en cause.

On trouve étonnante quand même le raisonnement de la juridiction européenne dans la présente affaire, vue qu'elle s'est rallie à l'importance quantitative des fichiers stockés et la rigueur dans l'appréciation de la situation et aussi à la dénomination que l'employé a utilisé pour relever que le contenu du fichier n'avait aucune connexion avec son travail- «personnel» et non «prive»., en accord avec la Charte de l'utilisateur: «La Cour, qui observe que les juridictions internes ont ainsi dûment examiné le moyen du requérant tiré d'une violation de

[18] (*https://www.legifrance.gouv.fr/affichCode.do?cidTexte=LEGITEXT000006072050*) consulte le 3 mars 2018.

son droit au respect de sa vie privée, juge ces motifs pertinents et suffisants. Certes, en usant du mot «personnel» plutôt que du mot «privé», le requérant a utilisé le même terme que celui que l'on trouve dans la jurisprudence de la Cour de cassation, selon laquelle l'employeur ne peut en principe ouvrir les fichiers identifiés par le salarié comme étant «personnels»[19].

V. Conclusions

Si l'arrêt monténégrin était prévisible, la décision espagnole est plus choquante, car la Cour va au-delà et s'immisce dans l'analyse très fine de la proportionnalité de la mesure pour conclure «qu'il aurait été possible de protéger au moins dans une certaine mesure les droits de l'employeur en recourant à d'autres moyens. L'entreprise aurait par exemple pu communiquer aux requérantes des informations générales sur la surveillance et procéder à la notification requise au titre de la loi sur la protection des données personnelles». Donc on pourrait apprécier que le message transmis par la juridiction européenne est le suivant: bien légitime que soit la finalité de la mesure-comme par exemple d'identifier des employés voleurs, le test de proportionnalité doit être réalisé avec le plus grand soucie.

On a donc pu noter qu'à deux reprises, la Cour est venu de s'opposer à la vidéosurveillance, y voyant une ingérence illicite et disproportionnée, même dans le cas où la surveillance a pour but d'identifier parmi les membres du personnel l'auteur de vols avérés, tout en estimant qu'il y avait des moyens plus appropries et moins intrusives pour concevoir la mesure, mais l'affaire Libert vient de montrer le contraire.

L'arrêt souligne en fait l'importance pour les entreprises de se doter d'instruments performants de régulation de l'usage des outils numériques, instruments comme la Charte de l'utilisateur –en l'absence de laquelle probablement le licenciement aurait été invalidé.

[19] CEDH, *Affaire Libert c. France*, n°588/13, 22 février 2018, §52.