



EUROPEAN COURT OF HUMAN RIGHTS
COUR EUROPÉENNE DES DROITS DE L'HOMME

GRANDE CHAMBRE

AFFAIRE BĂRBULESCU c. ROUMANIE

(Requête n° 61496/08)

ARRÊT

STRASBOURG

5 septembre 2017

Cet arrêt est définitif. Il peut subir des retouches de forme.

En l'affaire Bărbulescu c. Roumanie,

La Cour européenne des droits de l'homme, siégeant en une Grande Chambre composée de :

Guido Raimondi, *président*,
Angelika Nußberger,
Mirjana Lazarova Trajkovska, *juges*,
Luis López Guerra, *juge ad hoc*,
Ledi Bianku,
Işıl Karakaş,
Nebojša Vučinić,
André Potocki,
Paul Lemmens,
Dmitry Dedov,
Jon Fridrik Kjølbro,
Mărtiņš Mits,
Armen Harutyunyan,
Stéphanie Mourou-Vikström,
Georges Ravarani,
Marko Bošnjak,
Tim Eicke, *juges*,

et de Søren Prebensen, *greffier adjoint de la Grande Chambre*,

Après en avoir délibéré en chambre du conseil les 30 novembre 2016 et 8 juin 2017,

Rend l'arrêt que voici, adopté à cette dernière date :

PROCÉDURE

1. À l'origine de l'affaire se trouve une requête (n° 61496/08) dirigée contre la Roumanie et dont un ressortissant de cet État, M. Bogdan Mihai Bărbulescu (« le requérant »), a saisi la Cour le 15 décembre 2008 en vertu de l'article 34 de la Convention de sauvegarde des droits de l'homme et des libertés fondamentales (« la Convention »).

2. Le requérant a été représenté par M^{es} E. Domokos-Hâncu et O. Juverdeanu, avocats à Bucarest. Le gouvernement roumain (« le Gouvernement ») a été représenté par son agente, M^{me} C. Brumar, du ministère des Affaires étrangères.

3. Le requérant allègue en particulier que la décision de son employeur de mettre fin à son contrat de travail reposait sur une violation à son égard du droit au respect de la vie privée et de la correspondance garanti par l'article 8 de la Convention et que les juridictions internes ont manqué à leur obligation de protéger ce droit.

4. La requête a été attribuée à la quatrième section de la Cour (article 52 § 1 du règlement de la Cour – « le règlement »). Le 12 janvier 2016, une chambre de cette section, composée de András Sajó, président, Vincent A. De Gaetano, Boštjan M. Zupančič, Nona Tsotsoria, Paulo Pinto de Albuquerque, Egidijus Kūris et Iulia Motoc, juges, ainsi que de Fatoş Aracı, greffière adjointe de section, a déclaré, à l'unanimité, la requête recevable quant au grief tiré de l'article 8 de la Convention et irrecevable pour le surplus. Elle a conclu, par six voix contre une, à la non-violation de l'article 8 de la Convention. L'opinion dissidente du juge Pinto de Albuquerque a été jointe à l'arrêt de la chambre.

5. Le 12 avril 2016, le requérant a demandé le renvoi de l'affaire devant la Grande Chambre en vertu des articles 43 de la Convention et 73 du règlement. Le 6 juin 2016, le collège de la Grande Chambre a accueilli cette demande.

6. La composition de la Grande Chambre a été arrêtée conformément aux articles 26 §§ 4 et 5 de la Convention et 24 du règlement. À la suite du départ de Iulia Motoc, juge élue au titre de la Roumanie (article 28 du règlement), Luis López Guerra a été désigné par le président pour siéger en qualité de juge *ad hoc* (article 26 § 4 de la Convention et article 29 § 1 du règlement).

7. Tant le requérant que le Gouvernement ont déposé des observations écrites complémentaires (article 59 § 1 du règlement).

8. Des observations ont également été reçues du gouvernement français et de la Confédération européenne des syndicats, que le président avait autorisés à intervenir dans la procédure écrite (articles 36 § 2 de la Convention et 44 § 3 du règlement).

9. Une audience s'est déroulée en public au Palais des droits de l'homme, à Strasbourg, le 30 novembre 2016 (article 59 § 3 du règlement).

Ont comparu :

– *pour le Gouvernement*

M^{me} C. BRUMAR, *agente,*
M. G.V. GAVRILĂ, magistrat détaché à la direction
de l'Agent du Gouvernement, *conseil,*
M^{me} L.A. RUSU, ministre plénipotentiaire à la représentation
permanente de la Roumanie auprès du
Conseil de l'Europe, *conseillère ;*

– *pour le requérant*

M^{es} E. DOMOKOS-HÂNCU, avocat,
O. JUVERDEANU, avocat, *conseils.*

La Cour a entendu M^{es} Domokos-Hâncu et Juverdeanu, M^{me} Brumar et M. Gavrilă en leurs déclarations ainsi qu'en leurs réponses aux questions posées par des juges.

EN FAIT

I. LES CIRCONSTANCES DE L'ESPÈCE

10. Le requérant est né en 1979 et réside à Bucarest.

11. Du 1^{er} août 2004 au 6 août 2007, il fut employé au bureau de Bucarest de S., une société commerciale roumaine de droit privé (« l'employeur »), comme ingénieur chargé des ventes. À la demande de son employeur, il créa, pour répondre aux questions des clients, un compte de messagerie instantanée *Yahoo Messenger* (service de messagerie en ligne offrant une transmission de texte en temps réel sur internet). Il avait déjà un autre compte *Yahoo Messenger* personnel.

12. Le règlement intérieur de l'employeur prohibait l'usage par les employés des ressources de l'employeur, en ces termes :

Article 50

« Il est strictement interdit de troubler l'ordre et la discipline dans les locaux de l'entreprise, et en particulier :

(...)

- (...) d'utiliser les ordinateurs, les photocopieurs, les téléphones, les télécopieurs ou les télécopieurs à des fins personnelles. »

13. Ce règlement ne comportait par ailleurs aucune mention relative à la possibilité pour l'employeur de surveiller les communications de ses employés.

14. Il ressort des documents versés au dossier par le Gouvernement que le requérant avait été informé du règlement intérieur de l'employeur et l'avait signé, après avoir pris connaissance de son contenu, le 20 décembre 2006.

15. Le 3 juillet 2007, le bureau de Bucarest reçut et distribua à tous les employés une note d'information (« la note d'information ») rédigée et envoyée le 26 juin 2007 par le bureau central de Cluj. L'employeur demanda aux employés qu'ils prennent connaissance de cette note et qu'ils la signent. En ses parties pertinentes, la note est ainsi rédigée :

« 1. (...) Le temps passé dans l'entreprise doit être du temps de qualité pour tout le monde ! Venez au travail pour vous occuper des problèmes de l'entreprise, des problèmes professionnels, et pas de problèmes privés ! Ne passez pas votre temps à occuper les lignes d'internet, le téléphone ou le télécopieur avec des questions qui ne concernent ni le travail ni vos tâches. [L'éducation élémentaire], le bon sens et la loi

vous y obligent ! L'employeur se voit dans l'obligation de vérifier et de surveiller le travail des employés et de prendre des mesures de sanction envers les personnes en faute !

Vos fautes seront attentivement surveillées et réprimées !

2. En raison de fautes répétées [d'indiscipline commises] envers son supérieur, [ainsi que] de l'utilisation [qu'elle a faite] d'internet, du téléphone et du photocopieur à des fins privées, de sa négligence et du non-accomplissement de ses tâches, M^{elle} B.A. a été licenciée pour motifs disciplinaires ! Tirez les leçons de cet exemple négatif ! Ne commettez pas les mêmes erreurs !

3. Lisez attentivement la convention collective, le règlement interne de l'entreprise, le descriptif de votre poste et le contrat de travail que vous avez signé ! Ceux-ci sont la base de notre collaboration ! Celle entre l'employeur et l'employé ! (...) »

16. Il ressort également des documents versés au dossier par le Gouvernement, dont le registre de présence de l'employeur, que le requérant prit connaissance de cette note et la signa entre le 3 et le 13 juillet 2007.

17. Il en ressort par ailleurs que du 5 au 13 juillet 2007, l'employeur enregistra en temps réel les communications du requérant sur *Yahoo Messenger*.

18. Le 13 juillet 2007 à 16 heures 30, le requérant fut convoqué par son employeur. La convocation l'informait que ses communications sur *Yahoo Messenger* avaient été surveillées et qu'un certain nombre d'éléments indiquaient qu'il avait utilisé internet à des fins personnelles, contrairement au règlement intérieur. Y étaient joints des graphiques indiquant que son trafic internet était supérieur à celui de ses collègues. À ce stade, on ne l'informa pas si la surveillance de ses communications avait également visé leur contenu. La convocation était rédigée en ces termes :

« Vous devrez expliquer pourquoi vous utilisez à des fins personnelles les ressources de la société (connexion internet, *Messenger*) pendant les heures de travail, comme le montrent les graphiques ci-joints. »

19. Le même jour, le requérant répondit par écrit à l'employeur qu'il n'avait utilisé *Yahoo Messenger* qu'à des fins professionnelles.

20. À 17 heures 20, l'employeur le convoqua une seconde fois. La convocation était rédigée en ces termes :

« Expliquez pourquoi toute la correspondance que vous avez échangée entre le 5 et le 12 juillet 2007 en utilisant l'identifiant du site [internet] de S. Bucarest poursuit des buts privés, comme le démontrent les 45 pages ci-jointes. »

21. Les 45 pages mentionnées dans la convocation étaient la transcription de communications que le requérant avait eues avec son frère et sa fiancée pendant la période où il avait été surveillé ; ces communications portaient sur des questions privées et certaines avaient un caractère intime. La transcription comportait également cinq messages que le requérant avait échangés avec sa fiancée depuis son compte *Yahoo Messenger* personnel ; ces messages ne comportaient pas d'informations de nature intime.

22. Toujours le 13 juillet, le requérant informa par écrit son employeur qu'il l'estimait responsable de la commission d'une infraction pénale, à savoir la violation du secret de la correspondance.

23. Le 1^{er} août 2007, l'employeur mit fin au contrat de travail du requérant.

24. Le requérant contesta la décision de licenciement devant le tribunal départemental de Bucarest (« le tribunal départemental »). Il priait le tribunal, premièrement, d'annuler cette décision, deuxièmement, d'ordonner à son employeur de lui verser les sommes auxquelles il estimait avoir droit au titre de son salaire et d'autres créances et de le réintégrer à son poste et, troisièmement, de condamner l'employeur à lui payer des dommages-intérêts d'un montant de 100 000 lei roumains (environ 30 000 euros) au titre du préjudice moral qu'il estimait avoir subi du fait des modalités de son licenciement, et à lui rembourser ses frais et dépens.

25. Sur le fond, se fondant sur l'arrêt *Copland c. Royaume-Uni* (n° 62617/00, §§ 43-44, CEDH 2007-I), il arguait que les communications par téléphone ou par courrier électronique qu'un employé fait depuis son lieu de travail sont couvertes par les notions de « vie privée » et de « correspondance » et, dès lors, bénéficient de la protection de l'article 8 de la Convention. Il soutenait également que la décision de licenciement était illégale et qu'en surveillant ses communications et en accédant à leur contenu, son employeur avait enfreint la loi pénale.

26. Pour ce qui était en particulier du préjudice moral qu'il estimait avoir subi, le requérant rappelait la manière dont il avait été licencié et alléguait avoir subi de la part de son employeur un harcèlement qui s'était selon lui matérialisé par la surveillance de ses communications et par la divulgation de leur contenu « aux collègues impliqués d'une manière ou d'une autre dans la procédure de licenciement ».

27. Le requérant versa notamment au dossier à titre de preuves la copie intégrale des transcriptions de ses communications sur *Yahoo Messenger* ainsi qu'une copie de la note d'information (paragraphe 15 ci-dessus).

28. Par un jugement du 7 décembre 2007, le tribunal départemental rejeta l'action du requérant et confirma la licéité de la décision de licenciement. En ses parties pertinentes en l'espèce, ce jugement est ainsi libellé :

« La procédure relative à la conduite de l'enquête disciplinaire est expressément encadrée par les dispositions de l'article 267 du code du travail.

En l'espèce, il a été prouvé, par les documents écrits versés au dossier, que l'employeur a mené l'enquête disciplinaire contre le requérant en le convoquant par écrit à deux reprises [et] en précisant l'objet, la date, l'heure et le lieu de l'entretien, et que le requérant a eu la possibilité de présenter les arguments pour sa défense sur les faits qui lui étaient imputés, comme cela ressort du libellé des deux notes explicatives versées au dossier (en copie aux feuilles 89 et 91).

Le tribunal est d'avis que la surveillance des conversations que l'employé a échangées sur internet par l'intermédiaire du logiciel *Yahoo Messenger* depuis l'ordinateur de l'entreprise pendant les heures de bureau ne peut – indépendamment de la question de savoir si cette démarche de l'employeur était ou non illicite [du point de vue du droit] pénal – entacher la validité de la procédure disciplinaire menée en l'espèce.

La rédaction en termes impératifs des dispositions imposant d'entendre la personne soupçonnée d'un comportement fautif (*invinuitul*) et d'examiner les arguments qu'elle présente pour sa défense avant de décider d'une sanction montre que le législateur a entendu faire du respect des droits de la défense une condition de validité de la décision de sanction.

En l'espèce, dès lors que l'employé a affirmé dans le cadre de l'enquête disciplinaire ne pas avoir utilisé *Yahoo Messenger* à des fins personnelles mais aux fins de conseiller les clients sur les produits proposés par son employeur, le tribunal estime que la vérification de la teneur des communications [de l'intéressé] était le seul moyen pour l'employeur de vérifier la validité de ses arguments.

Le droit pour l'employeur de surveiller (*monitoriza*) les employés sur le lieu de travail, [en particulier] en ce qui concerne l'utilisation des ordinateurs de l'entreprise, relève du droit plus large de vérifier la manière dont les employés s'acquittent de leurs tâches professionnelles, qui est régi par les dispositions de l'article 40 d) du code du travail.

Dès lors qu'il a été prouvé que l'attention des employés avait été appelée sur le fait que, peu avant que le requérant ne fasse l'objet d'une sanction disciplinaire, une autre employée avait été licenciée pour avoir utilisé internet, le téléphone et le télécopieur à des fins personnelles, et qu'ils avaient été avertis que leurs activités étaient surveillées (voir la note n° 2316 du 3 juillet 2007, que le requérant avait signée [après en avoir] pris connaissance – en copie à la feuille 64), on ne peut accuser l'employeur de ne pas avoir fait preuve de transparence et de n'avoir pas clairement averti ses employés de la surveillance (*monitorizare*) qu'il opérait de leur usage des ordinateurs.

L'accès à internet sur le lieu de travail est avant tout un outil mis à la disposition de l'employé par l'employeur à des fins d'utilisation professionnelle et il est incontestable que l'employeur, en vertu de son droit de contrôler les activités de ses employés, a pour prérogative de contrôler l'usage personnel fait d'internet.

Ces vérifications de la part de l'employeur sont notamment rendues nécessaires par le risque que, par l'usage qu'ils font d'internet, les employés n'endommagent les systèmes informatiques de l'entreprise, ne se livrent à des activités illicites dans l'espace virtuel engageant la responsabilité de l'entreprise, ou ne révèlent des secrets industriels de l'entreprise.

Le tribunal est d'avis que les faits commis par le requérant révèlent une faute disciplinaire au sens des dispositions de l'article 263 § 2 du code du travail car ils constituent une transgression fautive des dispositions de l'article 50 du règlement interne de S. (...), qui prohibent l'utilisation des ordinateurs à des fins personnelles.

Les faits susmentionnés sont considérés en vertu du règlement interne comme une faute grave dont la sanction, conformément à l'article 73 du même règlement, [est] la rupture du contrat de travail pour motifs disciplinaires.

Eu égard aux arguments de fait et de droit déjà exposés, le tribunal conclut que la décision contestée est fondée et légale, et rejette l'action pour défaut de fondement. »

29. Le requérant contesta ce jugement devant la cour d'appel de Bucarest (« la cour d'appel »). Il répétait les arguments présentés devant la juridiction de premier ressort et soutenait en outre que celle-ci n'avait pas ménagé un juste équilibre entre les intérêts en jeu et avait injustement fait prévaloir l'intérêt de l'employeur à disposer discrétionnairement du temps et des ressources de ses employés. Il arguait également que ni le règlement intérieur ni la note d'information n'indiquaient que l'employeur pouvait surveiller les communications des employés.

30. La cour d'appel rejeta ce recours par un arrêt du 17 juin 2008. En ses parties pertinentes en l'espèce, cet arrêt est ainsi rédigé :

« C'est à bon droit que la juridiction de premier ressort a jugé qu'internet est un outil mis à la disposition de l'employé par l'employeur à des fins d'utilisation professionnelle et que l'employeur est en droit d'établir des règles pour l'utilisation de cet outil, en posant des interdictions et en adoptant des dispositions que les employés doivent respecter lorsqu'ils utilisent internet sur leur lieu de travail ; il est évident que l'utilisation à des fins personnelles peut être refusée, ce dont les employés ont été dûment informés en l'espèce par une note émise le 26 juin 2007 en application des dispositions du règlement intérieur et leur enjoignant de respecter les horaires de travail, d'être présents sur le lieu de travail [pendant ces horaires et] d'utiliser de manière efficace leur temps de travail.

En conclusion, l'employeur qui a fait un investissement est en droit, dans le contexte de l'exercice des droits prévus à l'article 40 § 1 du code du travail, de surveiller (*monitoriza*) l'utilisation faite d'internet sur le lieu de travail, et l'employé qui transgresse les règles de l'employeur relatives à l'utilisation d'internet à des fins personnelles commet une faute disciplinaire qui peut entraîner une sanction, notamment la sanction la plus grave.

Il est certain qu'entre le droit de surveillance (*monitorizarea*) de l'employeur et le droit des employés à la protection de leur vie privée, il existe un conflit. Celui-ci a été résolu au niveau de l'Union européenne par l'adoption de la directive 95/46/CE, qui a établi plusieurs principes régissant la surveillance (*monitorizarea*) de l'utilisation faite d'internet et du courrier électronique sur le lieu de travail, notamment les suivants.

- Principe de nécessité : la surveillance (*monitorizarea*) doit être nécessaire pour parvenir à un but donné.

- Principe de finalité : les données doivent être collectées à des fins spécifiques, explicites et légitimes.

- Principe de transparence : l'employeur doit fournir aux employés toutes les informations relatives à la surveillance (*monitorizare*).

- Principe de légitimité : les opérations de traitement des données ne peuvent avoir lieu que dans un but légitime.

- Principe de proportionnalité : les données personnelles qui font l'objet de la surveillance (*monitorizare*) doivent être pertinentes et adéquates par rapport au but indiqué.

- Principe de sécurité : l'employeur est tenu de prendre toutes les mesures de sécurité visant à garantir que les données collectées ne soient pas accessibles aux tiers.

Compte tenu du fait que l'employeur a le droit et l'obligation d'assurer le fonctionnement de l'entreprise et, à cette fin, [a le droit] de vérifier la manière dont

ses employés accomplissent leurs tâches professionnelles, et du fait [qu'il] a un pouvoir disciplinaire dont il peut légitimement faire usage et qui [lui donnait le droit en l'espèce] de surveiller et de retranscrire les communications sur *Yahoo Messenger* que l'employé n'ait avoir échangées à des fins personnelles après avoir été averti, comme ses collègues, qu'il ne devait pas utiliser les ressources de l'entreprise à des fins personnelles, on ne peut pas dire que la violation du secret de sa correspondance n'ait pas été la seule manière de parvenir à ce but légitime ni que le juste équilibre entre la nécessité de protéger la vie privée [de l'employé] et le droit pour l'employeur de superviser le fonctionnement de son entreprise n'ait pas été respecté.

(...)

Par voie de conséquence, au vu des éléments présentés ci-dessus, la cour juge que la décision de la juridiction de premier ressort est légale et fondée et que le recours est mal fondé ; il convient donc de le rejeter, en application des dispositions de l'article 312 § 1 du c[ode] de pr[océdure] civ[ile]. »

31. Entretemps, le 18 septembre 2007, le requérant déposa une plainte pénale contre les représentants légaux de S. pour violation du secret de la correspondance. Le 9 mai 2012, la direction des enquêtes sur la criminalité organisée et le terrorisme (« la DIICOT ») du parquet près la Haute Cour de cassation et de justice rendit une décision de non-lieu, au motif que l'entreprise était la propriétaire du système informatique et de la connexion internet et qu'elle pouvait dès lors contrôler le trafic internet de ses employés et utiliser les informations stockées sur le serveur et compte tenu de l'interdiction d'utiliser à des fins personnelles les systèmes informatiques, interdiction qui, à son avis, rendait prévisible la surveillance. Le requérant ne se prévalut pas de la possibilité que lui offraient les normes procédurales en vigueur, de contester la décision du parquet devant les juridictions internes.

II. LE DROIT INTERNE PERTINENT

A. La Constitution

32. En ses parties pertinentes, la Constitution roumaine dispose :

Article 26

« 1. Les autorités publiques respectent et protègent la vie intime, familiale et privée. »

Article 28

« Le secret des lettres, des télégrammes, des autres envois postaux, des conversations téléphoniques et des autres moyens légaux de communication est inviolable. »

B. Le code pénal

33. En ses parties pertinentes, le code pénal en vigueur au moment des faits se lisait ainsi :

Article 195 – Violation du secret de la correspondance

« 1. Quiconque, de manière illicite, ouvre la correspondance d'un tiers ou intercepte les conversations ou les communications téléphoniques d'un tiers, ses communications télégraphiques ou celles réalisées par tout autre moyen de transmission à longue distance est passible d'une peine d'emprisonnement de six mois à trois ans. »

C. Le code civil

34. Les dispositions pertinentes du code civil en vigueur au moment des faits étaient ainsi libellées :

Article 998

« Tout fait quelconque de l'homme qui cause à autrui un dommage oblige celui par la faute duquel il est arrivé à le réparer. »

Article 999

« Chacun est responsable du dommage qu'il a causé non seulement par son fait, mais encore par sa négligence ou par son imprudence. »

D. Le code du travail

35. Dans sa rédaction en vigueur au moment des faits, le code du travail, disposait :

Article 40

« 1. L'employeur a, en principe, les droits suivants :

(...)

d) contrôler la façon [dont les employés] accomplissent leurs tâches professionnelles ;

(...)

2. Il incombe à l'employeur, en principe, les obligations suivantes :

(...)

i) garantir la confidentialité des données à caractère personnel des employés. »

E. La loi n° 677/2001 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation des données à caractère personnel

36. En ses parties pertinentes, la loi n° 677/2001 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation des données à caractère personnel (« loi n° 677/2001 »), qui reprend certaines dispositions de la directive 95/46/CE du 24 octobre 1995 du Parlement européen et du Conseil de l'Union européenne, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (paragraphe 45 ci-dessous), se lit ainsi :

Article 3 – Définitions

« Aux fins de la présente loi, on entend par :

a) donnée à caractère personnel – toute information relative à une personne physique identifiée ou identifiable ; une personne identifiable est une personne qui peut être identifiée, directement ou indirectement, notamment par référence à un numéro d'identification ou à un ou plusieurs éléments spécifiques, propres à son identité physique, physiologique, psychique, économique, culturelle ou sociale ;

(...) »

Article 5 – Conditions de légitimité du traitement des données

« 1. Les données à caractère personnel (...) ne peuvent faire l'objet d'un quelconque traitement que si la personne concernée y a consenti de manière expresse et non équivoque.

2. Le consentement de la personne concernée n'est pas nécessaire dans les cas suivants :

a) lorsque le traitement est nécessaire à l'exécution d'un contrat auquel la personne concernée est partie ou à l'exécution de mesures précontractuelles prises à la demande de celle-ci ;

(...)

e) lorsque le traitement 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 ;

(...)

3. Les dispositions du paragraphe 2 sont sans préjudice des dispositions légales relatives à l'obligation pour les autorités publiques de respecter et de protéger la vie intime, familiale et privée. »

Article 18 – Droit de saisir la justice

« 1. Les personnes concernées ont le droit, sans préjudice de la possibilité d'adresser une plainte à l'autorité de surveillance, de saisir la justice pour obtenir la protection des droits garantis par la présente loi qui ont été enfreints.

2. Toute personne ayant subi un préjudice du fait du traitement illicite de ses données à caractère personnel peut saisir le tribunal compétent pour obtenir réparation [de son préjudice].

(...)»

III. LE DROIT INTERNATIONAL ET LA PRATIQUE INTERNATIONALE

A. Les normes des Nations Unies

37. Les principes directeurs pour la réglementation des fichiers personnels informatisés adoptés par l'Assemblée générale des Nations Unies le 14 décembre 1990 dans sa résolution 45/95 (A/RES/45/95) posent les garanties minimales qui devraient être prévues dans les législations nationales. Ils se lisent ainsi :

« 1. Principe de licéité et de loyauté

Les données concernant les personnes ne devraient pas être obtenues ou traitées à l'aide de procédés illicites ou déloyaux, ni utilisées à des fins contraires aux buts et aux principes de la Charte des Nations Unies.

2. Principe d'exactitude

Les personnes responsables de l'établissement d'un fichier ou celles responsables de [sa] mise en œuvre devraient être tenues de vérifier l'exactitude et la pertinence des données enregistrées et de veiller à ce qu'elles demeurent aussi complètes que possible pour éviter les erreurs par omission et qu'elles soient mises à jour, périodiquement ou lors de l'utilisation des informations contenues dans un dossier, tant qu'elles font l'objet d'un traitement.

3. Principe de finalité

La finalité en vue de laquelle est créé un fichier et son utilisation en fonction de cette finalité devraient être spécifiées, justifiées et, lors de sa mise en œuvre, faire l'objet d'une mesure de publicité ou être portées à la connaissance de la personne concernée, afin qu'il soit ultérieurement possible de vérifier :

- a) Si toutes les données personnelles collectées et enregistrées restent pertinentes par rapport à la finalité poursuivie ;
- b) Si aucune desdites données personnelles n'est utilisée ou divulguée, sauf accord de la personne concernée, à des fins incompatibles avec celles ainsi spécifiées ;
- c) Si la durée de conservation des données personnelles n'excède pas celle permettant d'atteindre la finalité pour laquelle elles ont été enregistrées.

4. Principe de l'accès par les personnes concernées

Toute personne justifiant de son identité a le droit de savoir si des données la concernant font l'objet d'un traitement, d'en avoir communication sous une forme intelligible, sans délais ou frais excessifs, d'obtenir les rectifications ou destructions adéquates en cas d'enregistrements illicites, injustifiés ou inexacts, et, lorsqu'elles sont communiquées, d'en connaître les destinataires. Une voie de recours devrait être prévue, le cas échéant, auprès de l'autorité de contrôle prévue au principe 8

ci-dessous. En cas de rectification, le coût devrait être à la charge du responsable du fichier. Il est souhaitable que les dispositions de ce principe s'appliquent à toute personne, quelle que soit sa nationalité ou sa résidence.

(...)

6. Faculté de dérogation

Des dérogations aux principes 1 à 4 ne peuvent être autorisées que si elles sont nécessaires pour protéger la sécurité nationale, l'ordre public, la santé ou la moralité publiques ainsi que, notamment, les droits et libertés d'autrui, spécialement de personnes persécutées (clause humanitaire), sous réserve que ces dérogations soient expressément prévues par la loi ou par une réglementation équivalente prise en conformité avec le système juridique interne qui en fixe expressément les limites et édicte des garanties appropriées.

(...)»

38. Le Bureau international du travail (BIT) a élaboré en 1997 un recueil de directives pratiques sur la protection des données personnelles des travailleurs (« le recueil de directives pratiques du BIT »), où sont énoncés les principes suivants :

« 5. Principes généraux

5.1. Les données personnelles devraient être traitées de manière licite et loyale et uniquement pour des raisons directement liées à l'emploi du travailleur.

5.2. En principe, les données personnelles ne devraient être utilisées qu'aux fins pour lesquelles elles ont été collectées à l'origine.

5.3. Si des données personnelles sont traitées à des fins autres que celles pour lesquelles elles ont été collectées, l'employeur devrait s'assurer que cela ne se fait pas d'une manière incompatible avec l'objectif premier de leur traitement et prendre toutes mesures nécessaires pour éviter les erreurs d'interprétation qui pourraient résulter de leur utilisation dans un autre contexte.

5.4. Les données personnelles collectées en relation avec la mise en œuvre de mesures techniques ou d'organisation visant à garantir la sécurité et le bon fonctionnement des systèmes d'information automatisés ne devraient pas servir à contrôler le comportement des travailleurs.

5.5. Les décisions relatives à un travailleur ne devraient pas se fonder exclusivement sur le traitement automatique des données personnelles le concernant.

5.6. Les données personnelles collectées par voie de surveillance électronique ne devraient pas être l'élément exclusif de l'évaluation des résultats du travailleur.

5.7. Les employeurs devraient procéder à une évaluation régulière de leurs méthodes de traitement des données afin :

a) de réduire au maximum les types et la quantité des données personnelles collectées ;

b) d'améliorer la protection de la vie privée des travailleurs.

5.8. Les travailleurs et leurs représentants devraient être tenus informés de tous mécanismes de collecte des données, des règles qui régissent ces mécanismes et de leurs droits.

(...)

5.13. Les travailleurs ne peuvent pas renoncer à leurs droits relatifs à la protection de leur vie privée. »

39. En ce qui concerne en particulier la surveillance des employés, le recueil de directives pratiques du BIT prévoit ceci :

« 6. Collecte des données personnelles

6.1. En principe, toutes les données personnelles devraient être obtenues du travailleur lui-même.

(...)

6.14. (1) Dans le cas où les travailleurs font l'objet d'une surveillance, ils devraient être informés à l'avance des raisons de cette surveillance, des périodes concernées, des méthodes et techniques utilisées, ainsi que des données collectées. L'employeur doit réduire à un minimum l'ingérence dans la vie privée des travailleurs.

(2) Toute surveillance secrète ne saurait être autorisée que :

a) si elle est conforme à la législation nationale ; ou

b) s'il existe des soupçons raisonnablement justifiés d'activités criminelles ou d'autres infractions graves.

(3) Toute surveillance permanente ne saurait être autorisée que pour des raisons de santé et de sécurité ou en vue de protéger les biens de l'entreprise. »

40. Le recueil dresse également un inventaire des droits individuels des employés, notamment en ce qui concerne l'information quant au traitement des données personnelles, à l'accès à ces données et au contrôle de ces mesures. Les parties pertinentes se lisent ainsi :

« 11. Droits individuels

11.1. Les travailleurs devraient avoir le droit d'être régulièrement informés des données personnelles les concernant et du traitement desdites données.

11.2. Les travailleurs devraient pouvoir consulter toutes les données personnelles les concernant, qu'elles soient traitées automatiquement, conservées dans un dossier concernant un travailleur donné ou dans tout autre dossier qui contient des données personnelles relatives au travailleur concerné.

11.3. Le droit d'un travailleur d'être au courant du traitement de ses données personnelles devrait inclure le droit d'examiner et d'obtenir une copie de tous les dossiers dans la mesure où les données qu'ils contiennent incluent les données personnelles de ce travailleur en particulier.

(...)

11.8. En cas d'enquête relative à la sécurité, l'employeur devrait avoir le droit de refuser au travailleur l'accès à ses données personnelles jusqu'à la clôture de l'enquête, dans la mesure où cet accès risquerait de nuire à celle-ci. Cependant, aucune décision concernant la relation d'emploi ne devrait être prise avant que le travailleur n'ait eu accès à l'ensemble des données personnelles.

11.9. Les travailleurs devraient avoir le droit d'exiger que les données personnelles incorrectes ou incomplètes, de même que les données personnelles qui ont été traitées

d'une manière non conforme aux dispositions du présent recueil, soient supprimées ou rectifiées.

(...)

11.13. Toutes législations, réglementations, conventions collectives, règles de travail ou politiques élaborées conformément aux dispositions du présent recueil devraient faire mention d'une possibilité de correction permettant au travailleur de contester le non-respect par l'employeur dudit recueil. Des procédures devraient être mises en place en vue de recevoir et de donner suite à toute plainte introduite par les travailleurs. La procédure de recours devrait être simple et facile d'accès pour les travailleurs. »

41. L'Assemblée Générale des Nations Unies a également adopté le 18 décembre 2013 la résolution n° 68/167 sur le droit à la vie privée à l'ère du numérique (A/RES/68/167), dans laquelle elle invite notamment les États :

« a) À respecter et à protéger le droit à la vie privée, notamment dans le contexte de la communication numérique ;

b) À prendre des mesures pour faire cesser les violations de ces droits et à créer des conditions qui permettent de les prévenir, notamment en veillant à ce que la législation nationale applicable soit conforme aux obligations que leur impose le droit international des droits de l'homme ;

c) À revoir leurs procédures, leurs pratiques et leur législation relatives à la surveillance et à l'interception des communications, et à la collecte de données personnelles, notamment à grande échelle, afin de défendre le droit à la vie privée en veillant à respecter pleinement toutes leurs obligations au regard du droit international ;

d) À créer des mécanismes nationaux de contrôle indépendants efficaces qui puissent assurer la transparence de la surveillance et de l'interception des communications et de la collecte de données personnelles qu'ils effectuent, le cas échéant, et veiller à ce qu'ils en répondent, ou à les maintenir en place s'ils existent déjà[.] »

B. Les normes du Conseil de l'Europe

42. La Convention du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (1981, STE n° 108), entrée en vigueur à l'égard de la Roumanie le 1^{er} juin 2002, prévoit en particulier ceci :

Article 2 – Définitions

« Aux fins de la présente Convention :

a) « données à caractère personnel » signifie : toute information concernant une personne physique identifiée ou identifiable (« personne concernée ») ;

(...)

c) « traitement automatisé » s'entend des opérations suivantes effectuées en totalité ou en partie à l'aide de procédés automatisés : enregistrement des données,

application à ces données d'opérations logiques et/ou arithmétiques, leur modification, effacement, extraction ou diffusion ;

(...) »

Article 3 – Champ d'application

« 1. Les Parties s'engagent à appliquer la présente Convention aux fichiers et aux traitements automatisés de données à caractère personnel dans les secteurs public et privé.

(...) »

Article 5 – Qualité des données

« Les données à caractère personnel faisant l'objet d'un traitement automatisé sont :

- a) obtenues et traitées loyalement et licitement ;
- b) enregistrées pour des finalités déterminées et légitimes et ne sont pas utilisées de manière incompatible avec ces finalités ;
- c) adéquates, pertinentes et non excessives par rapport aux finalités pour lesquelles elles sont enregistrées ;
- d) exactes et si nécessaire mises à jour ;
- e) conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire aux finalités pour lesquelles elles sont enregistrées. »

Article 8 – Garanties complémentaires pour la personne concernée

« Toute personne doit pouvoir :

- a) connaître l'existence d'un fichier automatisé de données à caractère personnel, ses finalités principales, ainsi que l'identité et la résidence habituelle ou le principal établissement du maître du fichier ;
- b) obtenir à des intervalles raisonnables et sans délais ou frais excessifs la confirmation de l'existence ou non dans le fichier automatisé de données à caractère personnel la concernant ainsi que la communication de ces données sous une forme intelligible ;

(...)

- d) disposer d'un recours s'il n'est pas donné suite à une demande de confirmation ou, le cas échéant, de communication, de rectification ou d'effacement, visée aux paragraphes b et c du présent article. »

Article 9 – Exceptions et restrictions

« (...)

2. Il est possible de déroger aux dispositions des articles 5, 6 et 8 de la présente Convention lorsqu'une telle dérogation, prévue par la loi de la Partie, constitue une mesure nécessaire dans une société démocratique :

- a) à la protection de la sécurité de l'État, à la sûreté publique, aux intérêts monétaires de l'État ou à la répression des infractions pénales ;

b) à la protection de la personne concernée et des droits et libertés d'autrui.

(...)»

Article 10 – Sanctions et recours

« Chaque Partie s'engage à établir des sanctions et recours appropriés visant les violations aux dispositions du droit interne donnant effet aux principes de base pour la protection des données énoncés dans le présent chapitre. »

43. La Recommandation 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, adoptée le 1^{er} avril 2015, énonce notamment ceci :

« 4. Application des principes de traitement des données

4.1. Les employeurs devraient veiller à ce que le traitement des données à caractère personnel ne porte que sur les données strictement nécessaires pour atteindre l'objectif déterminé dans les cas individuels concernés.

(...)

6. Utilisation interne des données

6.1. Les données à caractère personnel collectées à des fins d'emploi ne devraient être traitées par les employeurs qu'à de telles fins.

6.2. Les employeurs devraient adopter des politiques de protection des données, des règles et/ou d'autres instruments relatifs à l'usage interne des données à caractère personnel conformément aux principes de la présente recommandation.

(...)

10. Transparence du traitement

10.1. Des informations sur les données à caractère personnel détenues par des employeurs devraient être mises à la disposition de l'employé concerné, soit directement, soit par l'intermédiaire de ses représentants, ou être portées à sa connaissance par d'autres moyens appropriés.

10.2. Les employeurs devraient fournir à leurs employés les informations suivantes :

- les catégories de données qui seront traitées et une description des finalités du traitement ;
- les destinataires ou catégories de destinataires de ces données ;
- les moyens d'exercer les droits énoncés au principe 11 de la présente recommandation, sans pour autant porter préjudice à des moyens plus favorables prévus dans le droit interne ou le système législatif ;
- toute autre information nécessaire pour garantir un traitement loyal et licite des données.

10.3. Une description particulièrement claire et complète des catégories de données à caractère personnel qui peuvent être collectées au moyen de TIC, telle que la vidéosurveillance, et de leur utilisation potentielle, devrait être fournie. Ce principe vaut pour toutes les formes particulières de traitement de données à caractère personnel prévues à la partie II de l'annexe de la présente recommandation.

10.4. Les informations devraient être fournies sous une forme accessible et tenues à jour. Ces informations devraient, en tout état de cause, être fournies avant que l'employé exerce effectivement l'activité ou l'action prévue, et être mises à disposition au moyen des systèmes d'information habituellement utilisés par l'employé.

(...)

14. Utilisation de l'internet et des communications électroniques sur le lieu de travail

14.1. Les employeurs devraient éviter de porter des atteintes injustifiées et déraisonnables au droit au respect de la vie privée des employés. Ce principe s'étend à tous les dispositifs techniques et aux TIC utilisés par un employé. Les personnes concernées devraient être convenablement et périodiquement informées en application d'une politique claire en matière de respect de la vie privée, conformément au principe 10 de la présente recommandation. L'information fournie devrait être mise à jour et inclure la finalité du traitement, la durée de conservation des données collectées, la sauvegarde des données de connexion et l'archivage des messages électroniques professionnels.

14.2. En ce qui concerne plus particulièrement l'éventuel traitement de données à caractère personnel relatif aux pages internet ou intranet consultées par l'employé, il conviendrait de préférence d'une part d'adopter des mesures préventives, telles que la configuration de systèmes ou l'utilisation de filtres qui peuvent empêcher certaines opérations, et, d'autre part de prévoir éventuellement des contrôles des données à caractère personnel, effectués, de préférence, de manière graduée et par sondages non individuels, en utilisant des données anonymes ou, en quelque sorte, agrégées.

14.3. L'accès par des employeurs aux communications électroniques professionnelles de leurs employés, qui ont été informés au préalable de cette éventualité, ne peut survenir, le cas échéant, que si cela est nécessaire pour des raisons de sécurité ou pour d'autres raisons légitimes. En cas d'absence d'un employé, les employeurs devraient prendre les mesures nécessaires et prévoir les procédures appropriées visant à permettre l'accès aux communications électroniques professionnelles, uniquement lorsqu'un tel accès est nécessaire d'un point de vue professionnel. L'accès devrait intervenir de la façon la moins intrusive possible et uniquement après avoir informé les employés concernés.

14.4. En 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.

14.5. Lorsqu'un employé quitte son emploi, l'employeur devrait prendre des mesures techniques et organisationnelles afin que la messagerie électronique de l'employé soit désactivée automatiquement. Si le contenu de la messagerie devait être récupéré pour la bonne marche de l'organisation, l'employeur devrait prendre des mesures appropriées afin de récupérer son contenu avant le départ de l'employé et si possible en sa présence. »

IV. LE DROIT DE L'UNION EUROPÉENNE

44. Les dispositions pertinentes de la Charte des droits fondamentaux de l'Union européenne (2007/C 364/01) sont ainsi libellées :

Article 7 – Respect de la vie privée et familiale

« Toute personne a droit au respect de sa vie privée et familiale, de son domicile et de ses communications. »

Article 8 – Protection des données à caractère personnel

« 1. Toute personne a droit à la protection des données à caractère personnel la concernant.

2. Ces données doivent être traitées loyalement, à des fins déterminées et sur la base du consentement de la personne concernée ou en vertu d'un autre fondement légitime prévu par la loi. Toute personne a le droit d'accéder aux données collectées la concernant et d'en obtenir la rectification.

3. Le respect de ces règles est soumis au contrôle d'une autorité indépendante. »

45. La directive 95/46/CE du 24 octobre 1995 du Parlement européen et du Conseil de l'Union européenne, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (« la directive 95/46/CE »), énonce que l'objet des législations nationales relatives au traitement des données à caractère personnel est notamment d'assurer le respect du droit à la vie privée reconnu également à l'article 8 de la Convention et dans les principes généraux du droit communautaire. Ses dispositions pertinentes se lisent ainsi :

Article 2 – Définitions

« Aux fins de la présente directive, on entend par :

a) « données à caractère personnel » : toute information concernant une personne physique identifiée ou identifiable (personne concernée) ; est réputée identifiable une personne qui peut être identifiée, directement ou indirectement, notamment par référence à un numéro d'identification ou à un ou plusieurs éléments spécifiques, propres à son identité physique, physiologique, psychique, économique, culturelle ou sociale ;

(...) »

Article 6

1. Les États membres prévoient que les données à caractère personnel doivent être :

a) traitées loyalement et licitement ;

b) collectées pour des finalités déterminées, explicites et légitimes, et ne pas être traitées ultérieurement de manière incompatible avec ces finalités. Un traitement ultérieur à des fins historiques, statistiques ou scientifiques n'est pas réputé incompatible pour autant que les États membres prévoient des garanties appropriées ;

c) adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont collectées et pour lesquelles elles sont traitées ultérieurement ;

d) exactes et, si nécessaire, mises à jour ; toutes les mesures raisonnables doivent être prises pour que les données inexactes ou incomplètes, au regard des finalités pour

lesquelles elles sont collectées ou pour lesquelles elles sont traitées ultérieurement, soient effacées ou rectifiées ;

e) conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire à la réalisation des finalités pour lesquelles elles sont collectées ou pour lesquelles elles sont traitées ultérieurement. Les États membres prévoient des garanties appropriées pour les données à caractère personnel qui sont conservées au-delà de la période précitée, à des fins historiques, statistiques ou scientifiques.

2. Il incombe au responsable du traitement d'assurer le respect du paragraphe 1. »

Article 7

« Les États membres prévoient que le traitement de données à caractère personnel ne peut être effectué que si :

a) la personne concernée a indubitablement donné son consentement

ou

b) il est nécessaire à l'exécution d'un contrat auquel la personne concernée est partie ou à l'exécution de mesures précontractuelles prises à la demande de celle-ci

ou

c) il est nécessaire au respect d'une obligation légale à laquelle le responsable du traitement est soumis

ou

d) il est nécessaire à la sauvegarde de l'intérêt vital de la personne concernée

ou

e) il est nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique, dont est investi le responsable du traitement ou le tiers auquel les données sont communiquées

ou

f) il est 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, qui appellent une protection au titre de l'article 1^{er} paragraphe 1. »

Article 8 – Traitements portant sur des catégories particulières de données

« 1. Les États membres interdisent le traitement des données à caractère personnel qui révèlent l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques, l'appartenance syndicale, ainsi que le traitement des données relatives à la santé et à la vie sexuelle.

2. Le paragraphe 1 ne s'applique pas lorsque :

a) la personne concernée a donné son consentement explicite à un tel traitement, sauf dans le cas où la législation de l'État membre prévoit que l'interdiction visée au paragraphe 1 ne peut être levée par le consentement de la personne concernée

ou

b) 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

ou

c) le traitement est nécessaire à la défense des intérêts vitaux de la personne concernée ou d'une autre personne dans le cas où la personne concernée se trouve dans l'incapacité physique ou juridique de donner son consentement

ou

(...)

e) le traitement porte sur des données manifestement rendues publiques par la personne concernée ou est nécessaire à la constatation, à l'exercice ou à la défense d'un droit en justice.

(...)

4. Sous réserve de garanties appropriées, les États membres peuvent prévoir, pour un motif d'intérêt public important, des dérogations autres que celles prévues au paragraphe 2, soit par leur législation nationale, soit sur décision de l'autorité de contrôle. »

46. Un groupe de travail sur la protection des données (« le groupe de travail ») a été institué en vertu de l'article 29 de la directive. Selon l'article 30, il a pour mission :

« a) d'examiner toute question portant sur la mise en œuvre des dispositions nationales prises en application de la présente directive, en vue de contribuer à leur mise en œuvre homogène ;

b) de donner à la Commission un avis sur le niveau de protection dans la Communauté et dans les pays tiers ;

c) de conseiller la Commission sur tout projet de modification de la présente directive, sur tout projet de mesures additionnelles ou spécifiques à prendre pour sauvegarder les droits et libertés des personnes physiques à l'égard du traitement des données à caractère personnel, ainsi que sur tout autre projet de mesures communautaires ayant une incidence sur ces droits et libertés ;

d) de donner un avis sur les codes de conduite élaborés au niveau communautaire. »

Ce groupe est un organe consultatif de l'Union européenne et est indépendant. Il a rendu en septembre 2001 un avis sur le traitement des données à caractère personnel dans le contexte professionnel (avis 8/2001), où sont résumés les principes fondamentaux en matière de protection des données : finalité, transparence, légitimité, proportionnalité, exactitude, sécurité et information du personnel. Dans cet avis qu'il a adopté conformément à son mandat (contribuer à la mise en œuvre homogène des mesures nationales prises en application de la directive 95/46/CE), il a précisé que la surveillance des courriers électroniques impliquait un traitement des données à caractère personnel, et il a estimé que la surveillance des employés devait être

« une réponse proportionnée de l'employeur aux risques qu'il encourt de porter atteinte à la vie privée légitime et autres intérêts des salariés ».

47. En mai 2002, le groupe de travail a établi un document de travail concernant la surveillance des communications électroniques sur le lieu de travail (ci-après, « le document de travail »), dans lequel il tient compte expressément des dispositions de la directive 95/46/CE lue à la lumière des dispositions de l'article 8 de la Convention. Selon ce document, le simple fait qu'une activité de contrôle ou de surveillance soit considérée comme utile pour servir l'intérêt de l'employeur ne justifie pas à lui seul l'intrusion dans la vie privée du salarié, et toute mesure de surveillance doit répondre à quatre critères : transparence, nécessité, équité et proportionnalité.

48. En ce qui concerne l'aspect technique, le document de travail indique ceci :

« Des informations rapides peuvent aisément être affichées par un logiciel, par ex. des fenêtres d'avertissement qui préviennent le salarié que le système a détecté et/ou pris des mesures pour éviter une utilisation illicite du réseau. »

49. Plus spécifiquement, en ce qui concerne la question de l'accès aux e-mails des employés, le document comprend le passage suivant :

« La surveillance du courrier électronique ou de l'usage d'internet par un employé ne saurait être considérée [comme] nécessaire que dans des circonstances exceptionnelles. Par exemple, la surveillance du courrier électronique d'un employé peut apparaître nécessaire afin d'obtenir la confirmation ou la preuve de certaines actions de sa part. De telles actions devraient inclure une activité pénale de la part de l'employé pour autant qu'il soit nécessaire pour l'employeur de défendre ses propres intérêts, par exemple, lorsqu'il est responsable des actions de l'employé. Ces activités incluraient également la détection des virus et, en termes généraux, toute activité effectuée par l'employeur pour garantir la sécurité du système.

Il convient de mentionner que l'ouverture du courrier électronique d'un salarié peut également s'avérer nécessaire pour des raisons autres que le contrôle ou la surveillance, par exemple pour assurer la correspondance lorsque le salarié est absent (par ex. maladie ou vacances) ou que la correspondance ne peut pas être garantie autrement (par ex. via les fonctions de réponse ou de déviation automatique). »

50. La Cour de justice de l'Union européenne a interprété les dispositions de la directive 95/46/CE à la lumière du droit au respect de la vie privée tel que garanti par l'article 8 de la Convention dans l'affaire *Österreichischer Rundfunk et autres* (C-465/00, C-138/01 et C-139/01, arrêt du 20 mai 2003, ECLI:EU:C:2003:294, points 71 et suivants).

51. Le 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 (règlement général sur la protection des données), publié au JO 2016 L 119/1, est entré en vigueur le 24 mai 2016. Il abroge la directive 95/46/CE à compter du 25 mai 2018 (article 99). Ses dispositions pertinentes sont ainsi libellées :

Article 30 - Registre des activités de traitement

« 1. Chaque responsable du traitement et, le cas échéant, le représentant du responsable du traitement tiennent un registre des activités de traitement effectuées sous leur responsabilité. Ce registre comporte toutes les informations suivantes :

a) le nom et les coordonnées du responsable du traitement et, le cas échéant, du responsable conjoint du traitement, du représentant du responsable du traitement et du délégué à la protection des données ;

b) les finalités du traitement ;

c) une description des catégories de personnes concernées et des catégories de données à caractère personnel ;

d) les catégories de destinataires auxquels les données à caractère personnel ont été ou seront communiquées, y compris les destinataires dans des pays tiers ou des organisations internationales ;

e) le cas échéant, les transferts de données à caractère personnel vers un pays tiers ou à une organisation internationale, y compris l'identification de ce pays tiers ou de cette organisation internationale et, dans le cas des transferts visés à l'article 49, paragraphe 1, deuxième alinéa, les documents attestant de l'existence de garanties appropriées ;

f) dans la mesure du possible, les délais prévus pour l'effacement des différentes catégories de données ;

g) dans la mesure du possible, une description générale des mesures de sécurité techniques et organisationnelles visées à l'article 32, paragraphe 1.

2. Chaque sous-traitant et, le cas échéant, le représentant du sous-traitant tiennent un registre de toutes les catégories d'activités de traitement effectuées pour le compte du responsable du traitement, comprenant :

a) le nom et les coordonnées du ou des sous-traitants et de chaque responsable du traitement pour le compte duquel le sous-traitant agit ainsi que, le cas échéant, les noms et les coordonnées du représentant du responsable du traitement ou du sous-traitant et celles du délégué à la protection des données ;

b) les catégories de traitements effectués pour le compte de chaque responsable du traitement ;

c) le cas échéant, les transferts de données à caractère personnel vers un pays tiers ou à une organisation internationale, y compris l'identification de ce pays tiers ou de cette organisation internationale et, dans le cas des transferts visés à l'article 49, paragraphe 1, deuxième alinéa, les documents attestant de l'existence de garanties appropriées ;

d) dans la mesure du possible, une description générale des mesures de sécurité techniques et organisationnelles visées à l'article 32, paragraphe 1.

3. Les registres visés aux paragraphes 1 et 2 se présentent sous une forme écrite y compris la forme électronique.

4. Le responsable du traitement ou le sous-traitant et, le cas échéant, leur représentant mettent le registre à la disposition de l'autorité de contrôle sur demande.

5. Les obligations visées aux paragraphes 1 et 2 ne s'appliquent pas à une entreprise ou à une organisation comptant moins de 250 employés, sauf si le

traitement qu'elles effectuent est susceptible de comporter un risque pour les droits et des libertés des personnes concernées, s'il n'est pas occasionnel ou s'il porte notamment sur les catégories particulières de données visées à l'article 9, paragraphe 1, ou sur des données à caractère personnel relatives à des condamnations pénales et à des infractions visées à l'article 10. »

Article 47 - Règles d'entreprise contraignantes

« 1. L'autorité de contrôle compétente approuve des règles d'entreprise contraignantes conformément au mécanisme de contrôle de la cohérence prévu à l'article 63, à condition que :

- a) ces règles soient juridiquement contraignantes, et soient mises en application par toutes les entités concernées du groupe d'entreprises ou du groupe d'entreprises engagées dans une activité économique conjointe, y compris leurs employés ;
- b) elles confèrent expressément aux personnes concernées des droits opposables en ce qui concerne le traitement de leurs données à caractère personnel ; et
- c) elles répondent aux exigences prévues au paragraphe 2.

2. Les règles d'entreprise contraignantes visées au paragraphe 1 précisent au moins :

- a) la structure et les coordonnées du groupe d'entreprises ou du groupe d'entreprises engagées dans une activité économique conjointe et de chacune de leurs entités ;
- b) les transferts ou l'ensemble des transferts de données, y compris les catégories de données à caractère personnel, le type de traitement et ses finalités, le type de personnes concernées affectées et le nom du ou des pays tiers en question ;
- c) leur nature juridiquement contraignante, tant interne qu'externe ;
- d) l'application des principes généraux relatifs à la protection des données, notamment la limitation de la finalité, la minimisation des données, la limitation des durées de conservation des données, la qualité des données, la protection des données dès la conception et la protection des données par défaut, la base juridique du traitement, le traitement de catégories particulières de données à caractère personnel, les mesures visant à garantir la sécurité des données, ainsi que les exigences en matière de transferts ultérieurs à des organismes qui ne sont pas liés par les règles d'entreprise contraignantes ;
- e) les droits des personnes concernées à l'égard du traitement et les moyens d'exercer ces droits y compris le droit de ne pas faire l'objet de décisions fondées exclusivement sur un traitement automatisé, y compris le profilage, conformément à l'article 22, le droit d'introduire une réclamation auprès de l'autorité de contrôle compétente et devant les juridictions compétentes des États membres conformément à l'article 79 et d'obtenir réparation et, le cas échéant, une indemnisation pour violation des règles d'entreprise contraignantes ;
- f) l'acceptation, par le responsable du traitement ou le sous-traitant établi sur le territoire d'un État membre, de l'engagement de sa responsabilité pour toute violation des règles d'entreprise contraignantes par toute entité concernée non établie dans l'Union ; le responsable du traitement ou le sous-traitant ne peut être exonéré, en tout ou en partie, de cette responsabilité que s'il prouve que le fait générateur du dommage n'est pas imputable à l'entité en question ;

g) la manière dont les informations sur les règles d'entreprise contraignantes, notamment en ce qui concerne les éléments mentionnés aux points d), e) et f) du présent paragraphe sont fournies aux personnes concernées, en sus des informations visées aux articles 13 et 14 ;

h) les missions de tout délégué à la protection des données, désigné conformément à l'article 37, ou de toute autre personne ou entité chargée de la surveillance du respect des règles d'entreprise contraignantes au sein du groupe d'entreprises, ou du groupe d'entreprises engagées dans une activité économique conjointe, ainsi que le suivi de la formation et le traitement des réclamations ;

i) les procédures de réclamation ;

j) les mécanismes mis en place au sein du groupe d'entreprises, ou du groupe d'entreprises engagées dans une activité économique conjointe pour garantir que le contrôle du respect des règles d'entreprise contraignantes. Ces mécanismes prévoient des audits sur la protection des données et des méthodes assurant que des mesures correctrices seront prises pour protéger les droits de la personne concernée. Les résultats de ce contrôle devraient être communiqués à la personne ou à l'entité visée au point h) et au conseil d'administration de l'entreprise qui exerce le contrôle du groupe d'entreprises, ou du groupe d'entreprises engagées dans une activité économique conjointe, et devraient être mis à la disposition de l'autorité de contrôle compétente sur demande ;

k) les mécanismes mis en place pour communiquer et consigner les modifications apportées aux règles et pour communiquer ces modifications à l'autorité de contrôle ;

l) le mécanisme de coopération avec l'autorité de contrôle mis en place pour assurer le respect des règles par toutes les entités du groupe d'entreprises, ou du groupe d'entreprises engagées dans une activité économique conjointe, notamment en mettant à la disposition de l'autorité de contrôle les résultats des contrôles des mesures visés au point j) ;

m) les mécanismes permettant de communiquer à l'autorité de contrôle compétente toutes les obligations juridiques auxquelles une entité du groupe d'entreprises, ou du groupe d'entreprises engagées dans une activité économique conjointe, est soumise dans un pays tiers qui sont susceptibles d'avoir un effet négatif important sur les garanties fournies par les règles d'entreprise contraignantes ; et

n) la formation appropriée en matière de protection des données pour le personnel ayant un accès permanent ou régulier aux données à caractère personnel.

3. La Commission peut, pour les règles d'entreprise contraignantes au sens du présent article, préciser la forme de l'échange d'informations entre les responsables du traitement, les sous-traitants et les autorités de contrôle, ainsi que les procédures qui s'y rapportent. Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 93, paragraphe 2. »

Article 88 - Traitement de données dans le cadre des relations de travail

« 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. »

V. DROIT COMPARÉ

52. Il découle des documents dont la Cour dispose sur la législation des États membres du Conseil de l'Europe, notamment d'une étude portant sur trente-quatre États membres, que l'ensemble de ces États reconnaissent de manière générale, au niveau constitutionnel ou législatif, le droit au respect de la vie privée et au secret de la correspondance. Toutefois, seuls l'Autriche, la Finlande, le Luxembourg, le Portugal, le Royaume-Uni et la Slovaquie encadrent la question de l'exercice de la vie privée sur le lieu de travail de manière explicite, soit dans le cadre de la législation du travail, soit dans le cadre de lois spéciales.

53. En ce qui concerne les prérogatives de surveillance, trente-quatre États membres du Conseil de l'Europe exigent de l'employeur qu'il avertisse au préalable l'employé de la surveillance. Cet avertissement peut revêtir plusieurs formes, par exemple la notification aux autorités chargées de la protection des données à caractère personnel ou des représentants des employés. Les lois en vigueur en Autriche, en Estonie, en Finlande, en Grèce, en Lituanie, au Luxembourg, dans l'ex-République yougoslave de Macédoine, en Norvège, en Pologne et en Slovaquie exigent que l'employeur avertisse directement l'employé avant de commencer la surveillance.

54. En Allemagne, en Autriche, au Danemark, en Finlande, en France, en Grèce, en Italie, au Portugal et en Suède, les employeurs peuvent surveiller les courriers électroniques marqués par les employés comme « privés », sans toutefois pouvoir accéder à leur contenu. Au Luxembourg, l'employeur ne peut ouvrir ni les courriers marqués comme « privés » ni ceux qui le sont de toute évidence. L'Italie, la République tchèque et la Slovaquie, ainsi que, dans une certaine mesure, la République de Moldova imposent également des limitations au contrôle que l'employeur peut exercer sur les communications de ses employés, en fonction de la nature professionnelle ou personnelle de ces communications. En Allemagne et au

Portugal, une fois le caractère privé d'une communication établi, l'employeur doit cesser de la lire.

EN DROIT

I. SUR LA VIOLATION ALLÉGUÉE DE L'ARTICLE 8 DE LA CONVENTION

55. Le requérant soutient que la mesure de licenciement prise par son employeur reposait sur une violation à son égard du droit au respect de la vie privée et de la correspondance et que, dès lors qu'elles n'ont pas annulé cette mesure, les juridictions internes ont manqué à leur obligation de protéger ce droit. Il invoque l'article 8 de la Convention, qui est ainsi libellé :

« 1. Toute personne a droit au respect de sa vie privée et familiale, de son domicile et de sa correspondance.

2. Il ne peut y avoir ingérence d'une autorité publique dans l'exercice de ce droit que pour autant que cette ingérence est prévue par la loi et qu'elle constitue une mesure qui, dans une société démocratique, est nécessaire à la sécurité nationale, à la sûreté publique, au bien-être économique du pays, à la défense de l'ordre et à la prévention des infractions pénales, à la protection de la santé ou de la morale, ou à la protection des droits et libertés d'autrui. »

A. Les conclusions de la chambre

56. Dans son arrêt du 12 janvier 2016, la chambre a jugé, en premier lieu, que l'article 8 de la Convention était applicable en l'espèce. Se fondant sur la notion d'attente raisonnable en matière de respect de la vie privée, elle a estimé que la présente affaire se distinguait des affaires *Copland* (arrêt précité, § 41) et *Halford c. Royaume-Uni* (25 juin 1997, § 45, *Recueil des arrêts et décisions* 1997-III), dans la mesure où, en l'espèce, le règlement intérieur de l'entreprise interdisait strictement aux employés d'utiliser les ordinateurs et les ressources de l'entreprise à des fins personnelles. Elle a tenu compte de la nature des communications du requérant et du fait que leur transcription avait été utilisée comme élément de preuve dans le cadre de la procédure menée devant les juridictions internes, et elle a conclu que le droit du requérant au respect de sa « vie privée » et de sa « correspondance » était en jeu.

57. La chambre a ensuite situé son analyse sur le terrain des obligations positives de l'État, puisque la décision de licencier le requérant avait été prise par une personne de droit privé. Elle a donc recherché si les autorités nationales avaient 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.

58. Elle a noté que le requérant avait pu saisir les juridictions du travail et exposer devant elles ses arguments. Elle a observé que les tribunaux avaient jugé que le requérant avait commis une faute disciplinaire en utilisant internet à des fins personnelles pendant les heures de travail, et qu'ils avaient dans ce cadre pris en considération le déroulement de la procédure disciplinaire, notamment le fait que l'employeur n'avait eu accès au contenu des communications du requérant qu'après que ce dernier eut déclaré avoir utilisé *Yahoo Messenger* à des fins professionnelles.

59. Ensuite, la chambre a noté que les juridictions internes ne s'étaient pas appuyées dans leurs décisions sur le contenu des communications du requérant et que la surveillance opérée par l'employeur avait été limitée à l'usage que le requérant avait fait de *Yahoo Messenger*.

60. En conséquence, elle a conclu qu'il n'y avait pas eu violation de l'article 8 de la Convention.

B. Sur la portée de l'affaire devant la Grande Chambre

61. La Cour note que devant la chambre, le requérant alléguait que la décision de son employeur de mettre fin à son contrat de travail reposait sur une violation de son droit au respect de la vie privée et de la correspondance protégé par l'article 8 de la Convention, et que, dès lors qu'elles n'avaient pas annulé cette mesure, les juridictions internes avaient manqué à leur obligation de protéger ce droit. La chambre a déclaré ce grief recevable le 12 janvier 2016.

62. La Cour rappelle que l'affaire renvoyée devant la Grande Chambre est la requête telle qu'elle a été déclarée recevable par la chambre (*K. et T. c. Finlande* [GC], n° 25702/94, §§ 140-141, CEDH 2001-VII, *D.H. et autres c. République tchèque* [GC], n° 57325/00, § 109, CEDH 2007-IV, et *Blokhin c. Russie* [GC], n° 47152/06, § 91, CEDH 2016).

63. Dans ses observations devant la Grande Chambre, le requérant s'est plaint pour la première fois du rejet en 2012 de la plainte pénale qu'il avait déposée pour violation du secret de la correspondance (paragraphe 90 ci-dessous).

64. Ce nouveau grief n'est pas mentionné dans la décision de recevabilité du 12 janvier 2016, qui délimite le cadre de l'examen de la requête. Dès lors, il sort du champ d'examen de l'affaire telle qu'elle a été déférée à la Grande Chambre. Celle-ci n'est donc pas compétente pour en connaître, et elle limitera son examen au grief déclaré recevable par la chambre.

C. Sur l'applicabilité de l'article 8 de la Convention

1. Thèses des parties

a) Le Gouvernement

65. Le Gouvernement soutient que le requérant ne saurait prétendre qu'il pouvait croire au caractère « privé » des communications qu'il échangeait sur un compte de messagerie instantanée ouvert dans un but professionnel. Se fondant sur la jurisprudence des juridictions françaises et chypriotes, il soutient que les communications envoyées par un employé avec des moyens techniques mis à sa disposition par son employeur doivent être considérés comme ayant caractère professionnel, à moins que l'employé ne déclare expressément leur caractère privé. Il indique que *Yahoo Messenger* n'offre pas la possibilité technique de marquer une communication comme privée, mais que le requérant a toutefois eu une occasion adéquate, lors de la première phase de la procédure disciplinaire, de déclarer que ses communications étaient privées, et qu'il a néanmoins choisi de dire qu'elles étaient professionnelles. Il ajoute que le requérant avait été informé non seulement du règlement intérieur de son employeur, qui prohibait toute utilisation personnelle des ressources de l'entreprise, mais encore de ce que son employeur avait mis en place une surveillance de ses communications.

66. Le Gouvernement se fonde en outre sur un triple argument pour soutenir que l'article 8 de la Convention n'est pas applicable en l'espèce. Premièrement, il n'y aurait dans le dossier aucun élément permettant de dire que la transcription des communications du requérant ait été dévoilée à ses collègues de travail ; ce serait le requérant lui-même qui aurait produit la transcription intégrale de ces communications devant les juridictions internes, sans demander que l'accès à ces documents soit restreint. Deuxièmement, les autorités nationales auraient utilisé la transcription des communications comme élément de preuve parce que le requérant l'avait demandé et que les autorités pénales avaient déjà conclu à la licéité de la surveillance litigieuse des communications. Troisièmement, la note d'information aurait comporté des indications suffisantes pour que le requérant comprenne que son employeur pouvait surveiller ses communications, ce qui aurait ôté à celles-ci tout leur caractère privé.

b) Le requérant

67. Le requérant n'a pas présenté d'observations sur l'applicabilité de l'article 8 de la Convention, mais il a constamment soutenu que ses communications avaient un caractère privé.

68. Il a également argué que, ayant créé lui-même le compte *Yahoo Messenger* en question et étant seul à en connaître le mot de passe, il pouvait raisonnablement croire au caractère privé de ses communications. Il a aussi affirmé qu'il n'avait pas reçu de la part de son employeur de

notification relative à la mise en place de la surveillance de ses communications.

2. *Appréciation de la Cour*

69. La Cour note que se pose en l'espèce la question de savoir si les faits dont se plaint le requérant relèvent du champ d'application de l'article 8 de la Convention.

70. À ce stade de son examen, elle estime utile de rappeler que la notion de « vie privée » est une notion large, qui ne se prête pas à une définition exhaustive (*Sidabras et Džiautas c. Lituanie*, nos 55480/00 et 59330/00, § 43, CEDH 2004-VIII). L'article 8 de la Convention protège le droit à l'épanouissement personnel (*K.A. et A.D. c. Belgique*, nos 42758/98 et 45558/99, § 83, 17 février 2005), que ce soit sous la forme du développement personnel (*Christine Goodwin c. Royaume-Uni* [GC], n° 28957/95, § 90, CEDH 2002-VI) ou sous celle de l'autonomie personnelle, qui reflète un principe important sous-jacent dans l'interprétation des garanties de l'article 8 (*Pretty c. Royaume-Uni*, n° 2346/02, § 61, CEDH 2002-III). La Cour reconnaît que chacun a le droit de vivre en privé, loin de toute attention non voulue (*Smirnova c. Russie*, nos 46133/99 et 48183/99, § 95, CEDH 2003-IX (extraits)). Elle considère par ailleurs qu'il serait trop restrictif de limiter la notion de « vie privée » à un « cercle intime » où chacun peut mener sa vie personnelle à sa guise et d'en écarter entièrement le monde extérieur à ce cercle (*Niemietz c. Allemagne*, 16 décembre 1992, § 29, série A n° 251-B). Ainsi, l'article 8 garantit un droit à la « vie privée » au sens large, qui comprend le droit de mener une « vie privée sociale », à savoir la possibilité pour l'individu de développer son identité sociale. Sous cet aspect, ledit droit consacre la possibilité d'aller vers les autres afin de nouer et de développer des relations avec ses semblables (*Bigaeva c. Grèce*, n° 26713/05, § 22, 28 mai 2009, et *Özpinar c. Turquie*, n° 20999/04, § 45 *in fine*, 19 octobre 2010).

71. La Cour considère que la notion de « vie privée » peut inclure les activités professionnelles (*Fernández Martínez c. Espagne* [GC], n° 56030/07, § 110, CEDH 2014 (extraits), et *Oleksandr Volkov c. Ukraine*, n° 21722/11, §§ 165-166, CEDH 2013) ou les activités qui ont lieu dans un contexte public (*Von Hannover c. Allemagne (n° 2)* [GC], nos 40660/08 et 60641/08, § 95, CEDH 2012). 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. Il convient sur ce point de noter que c'est dans le cadre de leur travail que la majorité des gens ont beaucoup, voire le maximum, d'occasions de resserrer leurs liens avec le monde extérieur (*Niemietz*, précité, § 29).

72. Par ailleurs, pour ce qui est de la notion de « correspondance », il est à noter que, dans la rédaction de l'article 8 de la Convention, ce mot ne

s'accompagne d'aucun adjectif, contrairement au terme « vie ». La Cour a du reste déjà constaté qu'il n'y avait pas lieu de qualifier cette notion dans le cas de la correspondance téléphonique. Dans plusieurs affaires relatives à la correspondance avec un avocat, elle n'a pas même envisagé la possibilité que l'article 8 soit inapplicable du fait du caractère professionnel de la correspondance (voir en ce sens *Niemietz*, précité, § 32, avec les références citées). Elle a d'ailleurs conclu que les communications téléphoniques relèvent des notions de « vie privée » et de « correspondance » au sens de l'article 8 (*Roman Zakharov c. Russie* [GC], n° 47143/06, § 173, CEDH 2015). En principe, cela est également vrai lorsque ces communications émanent de locaux professionnels ou sont reçues dans de tels locaux (*Halford*, précité, § 44, et *Amann c. Suisse* [GC], n° 27798/95, § 44, CEDH 2000-II). Il en va de même pour les messages électroniques envoyés depuis le lieu de travail : ils relèvent aussi de la protection de l'article 8, tout comme les éléments recueillis au moyen d'une surveillance de l'usage qu'une personne fait d'internet (*Copland*, précité, § 41 *in fine*).

73. Il ressort clairement de la jurisprudence de la Cour que les communications émanant de locaux professionnels, tout comme celles provenant du domicile, peuvent se trouver comprises dans les notions de « vie privée » et de « correspondance » visées à l'article 8 de la Convention (*Halford*, précité, § 44 et *Copland*, précité, § 41). Afin de déterminer si les notions de « vie privée » et de « correspondance » sont applicables, la Cour a en plusieurs occasions recherché si l'individu pouvait raisonnablement s'attendre à ce que sa vie privée soit protégée et respectée (*ibidem* ; en ce qui concerne la « vie privée », voir *Köpke c. Allemagne* (déc.), n° 420/07, 5 octobre 2010). Dans ce contexte, elle a indiqué que l'attente raisonnable en matière de protection et de respect de la vie privée était un critère important, mais pas nécessairement décisif (*Köpke*, décision précitée).

74. Faisant application de ces principes en l'espèce, la Cour relève d'emblée que le type de messagerie instantanée sur internet en question n'est autre qu'une forme de communications faisant partie de l'exercice d'une vie privée sociale. Par ailleurs, la notion de « correspondance » s'applique à l'envoi et à la réception de messages, même depuis l'ordinateur de l'employeur. La Cour note toutefois que l'employeur du requérant attendait de ce dernier, ainsi que des autres employés, qu'ils s'abstiennent de toute activité personnelle sur leur lieu de travail. Cette exigence de l'employeur se traduisait notamment par une interdiction d'utiliser les ressources de l'entreprise à des fins personnelles (paragraphe 12 ci-dessus).

75. La Cour note ensuite que, en vue de s'assurer du respect de cette exigence, l'employeur a mis en place un système de surveillance de l'usage que ses employés faisaient d'internet (paragraphe 17 et 18 ci-dessus). Il ressort des documents versés au dossier, notamment de ceux relatifs à la procédure disciplinaire dirigée contre le requérant, que lors de cette activité de surveillance, tant les flux que le contenu des communications du

requérant ont été enregistrés et sauvegardés (paragraphe 18 et 20 ci-dessus).

76. La Cour remarque également que, malgré cette exigence de l'employeur, le requérant a échangé des communications de nature personnelle avec sa fiancée et son frère (paragraphe 21 ci-dessus). Certaines de ces communications avaient un caractère intime (*ibidem*).

77. La Cour est d'avis qu'il ressort clairement du dossier que le requérant avait bien été informé de l'interdiction d'utiliser internet à des fins personnelles posée par le règlement intérieur de son employeur (paragraphe 14 ci-dessus). Toutefois, il n'est pas aussi clair qu'il ait été informé que ses communications étaient surveillées avant que l'activité de surveillance ne soit mise en place. Ainsi, le Gouvernement soutient que le requérant a pris connaissance de la note d'information de l'employeur à une date non précisée entre le 3 et le 13 juillet 2007 (paragraphe 16 ci-dessus). Or les autorités nationales ont omis de rechercher si le requérant avait été informé de l'activité de surveillance à une date antérieure à la date de la mise en place de celle-ci étant donné que l'employeur a enregistré les communications en temps réel du 5 au 13 juillet 2007 (paragraphe 17 ci-dessus).

78. Quoi qu'il en soit, il n'apparaît pas que le requérant ait été informé à l'avance de l'étendue et de la nature de la surveillance opérée par son employeur ni de la possibilité que celui-ci ait accès à la teneur même de ses communications.

79. La Cour prend note également de l'argument du requérant selon lequel il avait créé lui-même le compte *Yahoo Messenger* en question et était seul à en connaître le mot de passe (paragraphe 68 ci-dessus). De plus, elle constate qu'il ressort des éléments versés au dossier que l'employeur a également eu accès au compte *Yahoo Messenger* personnel du requérant (paragraphe 21 ci-dessus). Cela étant, le requérant avait créé le compte *Yahoo Messenger* en question sur les instructions de son employeur pour répondre aux questions des clients (paragraphe 11 ci-dessus), et l'employeur y a eu accès.

80. 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. Cela étant, les instructions d'un employeur ne peuvent 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.

81. À la lumière de l'ensemble de ces considérations, la Cour conclut que les communications que le requérant a effectuées depuis son lieu de travail étaient couvertes par les notions de « vie privée » et de « correspondance ». Il s'ensuit que, compte tenu des circonstances, l'article 8 de la Convention est applicable en l'espèce.

D. Sur le respect de l'article 8 de la Convention

1. Thèses des parties et observations des tiers intervenants

a) Le requérant

82. Dans les observations écrites qu'il a soumises à la Grande Chambre, le requérant soutient que la chambre n'a pas suffisamment pris en considération certains éléments factuels de l'affaire. Premièrement, il insiste sur les spécificités de *Yahoo Messenger*, outil qui serait conçu pour un usage personnel. Il considère que le choix fait par son employeur d'utiliser cet outil dans le cadre professionnel ne saurait changer le fait qu'il est fondamentalement destiné à des fins personnelles. Il estime ainsi être le seul propriétaire du compte *Yahoo Messenger* qu'il a ouvert à la demande de son employeur.

83. Deuxièmement, le requérant argue que son employeur n'avait pas mis en place de politique d'utilisation d'internet. Il allègue n'avoir été aucunement averti de la possibilité que ses communications soient surveillées ou lues. Il affirme également ne pas avoir donné son accord à cette fin. Il indique que si une telle politique avait été en place et qu'il en avait été informé, il se serait abstenu d'exposer certains aspects de sa vie privée sur *Yahoo Messenger*.

84. Troisièmement, le requérant estime qu'il convient de faire une distinction entre l'utilisation d'internet à des fins personnelles ayant pour but un profit matériel et « une simple conversation courte et inoffensive » qui ne visait pas le profit et qui n'aurait causé aucun préjudice à l'employeur – à cet égard, il fait valoir que ce dernier ne lui a d'ailleurs pas reproché lors de la procédure disciplinaire d'avoir causé un préjudice à l'entreprise. Le requérant insiste sur l'évolution des technologies de l'information et de la communication et sur celle des mœurs et des usages sociaux à cet égard. Il est d'avis que les circonstances qui prévalent actuellement dans le monde du travail ne permettent pas de tracer une ligne de démarcation nette entre vie professionnelle et vie privée, et il estime illégitime toute politique managériale interdisant l'usage à des fins personnelles d'internet et des dispositifs connexes.

85. Sur le plan juridique, le requérant considère que l'État roumain n'a pas respecté les obligations positives que lui impose l'article 8 de la Convention. Plus précisément, il se plaint que les juridictions internes n'aient pas annulé son licenciement, alors qu'elles avaient selon lui reconnu la violation de son droit au respect de ses communications privées.

86. Il soutient en premier lieu que c'est à tort que la chambre a distingué la présente affaire de l'arrêt *Copland* (précité, § 42). Selon lui, l'élément déterminant pour l'analyse n'est pas le fait que l'employeur ait toléré ou non l'usage d'internet à des fins personnelles, mais le fait qu'il n'ait pas averti l'employé que ses communications pouvaient être surveillées. À cet égard,

il argue que son employeur l'a d'abord mis sous surveillance et qu'il ne lui a donné qu'ensuite l'occasion de préciser si ses communications étaient privées ou professionnelles. Il soutient qu'il faut examiner les questions de savoir, d'une part, si le fait d'avoir interdit totalement l'usage d'internet à des fins personnelles donne à l'employeur le droit de surveiller ses employés et, d'autre part, si l'employeur doit motiver la surveillance.

87. En second lieu, le requérant estime que l'analyse faite par la chambre sous l'angle du second paragraphe de l'article 8 n'est pas conforme à la jurisprudence de la Cour : elle n'aurait pas recherché si l'ingérence portée dans son droit au respect de sa vie privée et de sa correspondance était prévue par la loi, si elle poursuivait un but légitime et si elle était nécessaire dans une société démocratique.

88. En ce qui concerne la compétence des juridictions du travail, le requérant affirme que celles-ci peuvent exercer un contrôle complet de la légalité et du bien-fondé de la mesure soumise à leur examen. Selon lui, il revient au juge de demander la production des éléments de preuve nécessaires et de soulever toute question de fait ou de droit pertinente, même si les parties n'en font pas mention. Ainsi, les juridictions du travail auraient une compétence étendue pour examiner toute question relative à un litige de droit du travail, y compris les questions liées au respect de la vie privée et de la correspondance des employés.

89. Pourtant, l'approche des juridictions nationales dans son cas aurait été rigide et n'aurait visé qu'à confirmer la décision de son employeur. Les juges roumains auraient fait une analyse erronée des éléments factuels de l'affaire et n'auraient pas pris en compte les spécificités des communications dans le monde virtuel. Ainsi, la violation du droit du requérant au respect de sa vie privée et de sa correspondance aurait été intentionnelle et illégale et aurait eu pour but de produire des éléments de preuve permettant de mettre fin à son contrat de travail.

90. Enfin, le requérant se plaint pour la première fois dans le cadre de la procédure devant la Grande Chambre de l'issue de la plainte pénale qu'il a déposée en 2007 : en 2012, la direction des enquêtes sur la criminalité organisée et le terrorisme (DIICOT) du parquet aurait rejeté cette plainte sans avoir correctement établi les faits de l'affaire.

91. Lors de l'audience devant la Grande Chambre, le requérant a indiqué, en réponse à une question posée par les juges, que, du fait que son employeur ne mettait à la disposition des employés qu'une seule et unique imprimante, tous ses collègues auraient pu consulter le contenu des quarante-cinq pages de transcriptions de ses communications sur *Yahoo Messenger*.

92. Le requérant invite la Grande Chambre à conclure à la violation de l'article 8 de la Convention et à confirmer à cette occasion que la surveillance de la correspondance des employés ne peut se faire que dans le respect des lois en vigueur, de manière transparente et pour les raisons

prévues par la loi, et que l'employeur ne dispose pas d'un pouvoir discrétionnaire de surveiller la correspondance de ses employés.

b) Le Gouvernement

93. Le Gouvernement indique que l'employeur a enregistré les communications du requérant du 5 au 13 juillet 2007 et lui a ensuite donné la possibilité de s'expliquer sur l'usage qu'il avait fait d'internet, usage qui aurait été plus important que celui de ses collègues. Il explique que, le requérant ayant prétendu que le contenu de ses communications était professionnel, l'employeur a vérifié ses explications.

94. Il argue que le requérant n'a pas contesté dans son recours contre la décision rendue par la juridiction de premier ressort la conclusion des juges selon laquelle il avait été informé que son employeur surveillait l'usage fait d'internet. À cet égard, il verse au dossier une copie de la note d'information de l'employeur, signée par le requérant. Se fondant sur le registre de présence de l'employeur, il soutient que le requérant a signé cette note entre le 3 et le 13 juillet 2007.

95. Le Gouvernement expose également que l'employeur a enregistré en temps réel les communications du requérant. Il estime qu'il ne ressort pas du dossier que l'employeur ait eu accès à des communications antérieures ni au courrier électronique privé du requérant.

96. Le Gouvernement fait siennes les conclusions de la chambre et soutient que l'État roumain a respecté les obligations positives que lui impose l'article 8 de la Convention.

97. Il relève d'emblée que le requérant a choisi de soumettre ses griefs aux juridictions nationales dans le cadre d'une procédure de droit du travail. Il argue que les tribunaux ont examiné tous ces griefs et mis en balance les différents intérêts en jeu, mais que l'objet principal de leur analyse était la conformité au droit interne de la procédure disciplinaire dirigée contre le requérant. Celui-ci aurait eu la possibilité de saisir les juridictions nationales de son grief spécifique tiré de la violation de son droit au respect de sa vie privée, notamment dans le cadre d'une action fondée sur les dispositions de la loi n° 677/2001 ou d'une action en responsabilité civile délictuelle, mais il aurait choisi de ne pas le faire. Il aurait par ailleurs déposé une plainte pénale, sur laquelle le parquet aurait rendu une décision de non-lieu au motif que la surveillance par l'employeur des communications de ses employés n'avait pas été illégale.

98. Pour ce qui est plus particulièrement des obligations positives de l'État, le Gouvernement expose qu'il existe une grande variété d'approches parmi les États membres du Conseil de l'Europe quant à la réglementation de la surveillance que les employeurs peuvent exercer sur leurs employés. Certains États incluraient cette question dans celle plus large du traitement des données personnelles, alors que d'autres auraient adopté une législation spécifique à cet égard. Même au sein de ce second groupe d'États, les

solutions adoptées ne seraient pas uniformes quant à l'étendue et à la finalité de la surveillance de l'employeur, à l'avertissement préalable des employés ou à l'utilisation d'internet à des fins personnelles.

99. S'appuyant sur la décision *Köpke* précitée, le Gouvernement soutient que les juridictions nationales ont correctement mis en balance le droit du requérant au respect de sa vie privée et de sa correspondance et celui pour son employeur d'organiser et de superviser le travail dans son entreprise. Selon lui, lorsque la surveillance des communications est le fait d'une personne privée, un examen adéquat par les autorités nationales est suffisant aux fins de l'article 8 et un système normatif spécifique de protection n'est pas nécessaire.

100. Le Gouvernement argue ensuite que les juridictions nationales ont examiné la légalité et la nécessité de la décision de l'employeur et ont conclu que la procédure disciplinaire avait été menée conformément aux lois en vigueur. Il attache une importance particulière à la façon dont cette procédure a été menée, en particulier quant à la possibilité offerte au requérant d'indiquer si les communications en cause avaient un caractère privé. Selon lui, si le requérant avait fait usage de cette possibilité, les tribunaux auraient mis en balance différemment les intérêts en jeu.

101. À cet égard, le Gouvernement souligne que dans la procédure menée devant les autorités nationales, c'est le requérant lui-même qui a produit la copie intégrale des transcriptions de ses communications, sans prendre aucune précaution ; il soutient que le requérant aurait pu n'indiquer que les noms des comptes en question ou soumettre des extraits de ses communications, notamment celles qui ne comportaient pas d'informations de nature intime. Il conteste également les allégations du requérant selon lesquelles ses communications auraient été divulguées à ses collègues et il précise que seul le comité de discipline composé de trois personnes y a eu accès.

102. Le Gouvernement estime par ailleurs que la décision de l'employeur était nécessaire : celui-ci aurait dû vérifier les arguments avancés par le requérant dans le cadre de la procédure disciplinaire pour déterminer si l'intéressé avait respecté le règlement intérieur.

103. Enfin, le Gouvernement est d'avis qu'il faut faire une distinction entre la nature des communications et leur contenu. Il observe, comme la chambre, que les juridictions nationales n'ont aucunement tenu compte du contenu des communications du requérant mais se sont limitées à examiner leur nature et ont conclu qu'elles étaient personnelles.

104. Le Gouvernement conclut donc que le grief que le requérant tire de l'article 8 de la Convention n'est pas fondé.

c) Les tiers intervenants*i. Le gouvernement français*

105. Le gouvernement français expose, en particulier, sa conception de l'étendue de l'obligation positive pour les autorités nationales d'assurer le respect de la vie privée et de la correspondance des employés. Il procède à une présentation exhaustive des dispositions de droit civil, de droit du travail et de droit pénal français applicables en la matière. À son avis, l'article 8 de la Convention n'est applicable que pour les données, correspondances et activités électroniques strictement personnelles. À cet égard, il se fonde sur une jurisprudence constante de la Cour de cassation française, selon laquelle les données traitées, adressées et reçues par la voie d'un matériel électronique professionnel sont présumées avoir un caractère professionnel, sauf si l'employé les désigne, de manière claire et précise, comme personnelles.

106. Le gouvernement français est d'avis que la marge d'appréciation dont jouissent les États en cette matière doit être ample, puisqu'il s'agit de ménager un équilibre entre des intérêts privés concurrents. Il estime que l'employeur peut exercer une surveillance raisonnable des données et correspondances professionnelles des employés, pour autant qu'elle poursuive un but légitime, et utiliser le résultat de cette surveillance dans le cadre d'une procédure disciplinaire. Il souligne que la surveillance doit s'accompagner d'une information préalable des employés à cet égard. Enfin, il indique que lorsque sont en jeu des données clairement désignées par l'employé comme personnelles, l'employeur peut saisir les tribunaux afin que ceux-ci ordonnent des mesures d'instruction et qu'ils mandatent un huissier de justice pour accéder aux données en question et consigner leur contenu.

ii. La Confédération européenne des syndicats

107. La Confédération européenne des syndicats estime qu'il est crucial de protéger le droit au respect de la vie privée dans le cadre des relations de travail, compte tenu notamment de la dépendance structurelle des employés vis-à-vis des employeurs. Après avoir rappelé les principes de droit international et européen applicables, elle indique que l'accès à internet devrait être considéré comme un droit de l'homme et que le droit au respect de la correspondance devrait être renforcé. À son avis, le consentement des employés ou au moins leur information préalable, ainsi que l'information de leurs représentants, sont requis pour que l'employeur puisse traiter leurs données personnelles.

2. *Appréciation de la Cour*

a) **Sur la question de savoir si l'affaire concerne une obligation négative ou une obligation positive**

108. La Cour doit rechercher si la présente affaire doit être examinée sous l'angle des obligations négatives ou des obligations positives de l'État. Elle rappelle qu'aux termes de l'article 1 de la Convention, les États contractants « reconnaissent à toute personne relevant de leur juridiction les droits et libertés définis (...) [dans] la (...) Convention ». Si l'article 8 de la Convention a essentiellement pour objet de prémunir l'individu contre des ingérences arbitraires des pouvoirs publics, il peut également imposer à l'État des obligations positives inhérentes à un respect effectif des droits qu'il garantit (voir, parmi d'autres, *X et Y c. Pays-Bas*, 26 mars 1985, § 23, série A n° 91, *Von Hannover (n° 2)*, précité, § 98, et *Hämäläinen c. Finlande* [GC], n° 37359/09, § 62, CEDH 2014).

109. En l'espèce, la Cour observe que la mesure contestée par le requérant, à savoir la surveillance des communications échangées sur *Yahoo Messenger* qui a entraîné l'ouverture contre lui d'une procédure disciplinaire, puis son licenciement, pour non-respect des règles internes prohibant l'usage des ressources de l'entreprise à des fins personnelles fixées par son employeur, a été prise non pas par une autorité étatique, mais par une société commerciale de droit privé. La surveillance des communications du requérant par l'employeur et la consultation que ce dernier a faite de leur contenu en vue de justifier le licenciement de l'intéressé ne sauraient donc s'analyser en une « ingérence » dans le droit de celui-ci par une autorité de l'État.

110. Néanmoins, la Cour note que la mesure prise par l'employeur a été validée par les juridictions nationales. Il est vrai que la surveillance des communications du requérant ne résultait pas d'une intervention directe des autorités nationales mais pour autant, la responsabilité de ces autorités serait engagée si les faits litigieux résultaient d'un manquement de leur part à garantir au requérant la jouissance d'un droit consacré par l'article 8 de la Convention (voir, *mutatis mutandis*, *Obst c. Allemagne*, n° 425/03, §§ 40 et 43, 23 septembre 2010, et *Schüth c. Allemagne*, n° 1620/03, §§ 54 et 57, CEDH 2010).

111. Compte tenu des circonstances particulières de l'espèce, telles que décrites au paragraphe 109 ci-dessus, la Cour juge, à la lumière de sa conclusion relative à l'applicabilité de l'article 8 de la Convention (paragraphe 81 ci-dessus) et compte tenu de ce que l'atteinte à l'exercice par le requérant de son droit au respect de sa vie privée et de sa correspondance a été le fait d'un employeur privé, qu'il y a lieu d'analyser le grief sous l'angle des obligations positives de l'État.

112. Si la frontière entre les obligations positives et les obligations négatives de l'État au regard de la Convention ne se prête pas à une

définition précise, les principes applicables sont néanmoins comparables. En particulier, dans les deux cas, il faut prendre en compte le juste équilibre à ménager entre l'intérêt général et les intérêts de l'individu, l'État jouissant en toute hypothèse d'une marge d'appréciation (*Palomo Sánchez et autres c. Espagne* [GC], nos 28955/06 et 3 autres, § 62, CEDH 2011).

b) Les principes généraux applicables à l'appréciation de l'obligation positive pour l'État d'assurer le respect de la vie privée et de la correspondance dans le cadre des relations de travail

113. La Cour rappelle que le choix des mesures propres à garantir l'observation de l'article 8 dans les rapports interindividuels relève en principe de la marge d'appréciation des États contractants. Il existe en effet différentes manières d'assurer le respect de la vie privée, et la nature de l'obligation de l'État dépend de l'aspect de la vie privée qui se trouve en cause (*Söderman c. Suède* [GC], n° 5786/08, § 79, CEDH 2013, avec les références citées).

114. En l'espèce, il revient donc à la Cour de préciser la nature et l'étendue des obligations positives de l'État défendeur, auquel il incombait de protéger le droit du requérant au respect de sa vie privée et de sa correspondance dans le cadre de ses relations de travail.

115. La Cour rappelle qu'elle a conclu que, dans certaines circonstances, l'État ne s'acquitte de manière adéquate des obligations positives que lui impose l'article 8 de la Convention que s'il assure le respect de la vie privée dans les relations entre individus en établissant un cadre normatif qui prenne en considération les divers intérêts à protéger dans un contexte donné (*X et Y c. Pays-Bas*, précité, §§ 23, 24 et 27, et *M.C. c. Bulgarie*, n° 39272/98, § 150, CEDH 2003-XII, affaires concernant toutes deux des agressions sexuelles sur des mineurs ; voir également *K.U. c. Finlande*, n° 2872/02, §§ 43 et 49, CEDH 2008, affaire relative à une annonce de nature sexuelle publiée au nom d'un mineur sur un site de rencontres par internet, *Söderman*, précité, § 85, concernant l'effectivité des voies de recours au sujet d'une plainte pour atteinte à l'intégrité personnelle commise par un parent proche, et *Codarcea c. Roumanie*, n° 31675/04, §§ 102-104, 2 juin 2009, concernant des négligences médicales).

116. La Cour admet que des mesures protectrices peuvent être prévues tant par le droit du travail que par le droit civil et le droit pénal. En ce qui concerne le droit du travail, elle doit rechercher si, en l'espèce, l'État défendeur était tenu d'adopter un cadre normatif visant à protéger le droit du requérant au respect de sa vie privée et de sa correspondance dans le contexte de ses relations de travail avec un employeur privé.

117. À cet égard, elle relève que le droit du travail présente des caractéristiques spécifiques qui doivent être prises en compte. La relation entre un employeur et son employé est une relation contractuelle, assortie pour chacun de droits et d'obligations particulières, et caractérisée par un

lien de subordination légale. Elle est régie par un régime juridique propre, qui se distingue nettement du régime général des relations entre individus (*Saumier c. France*, n° 74734/14, § 60, 12 janvier 2017).

118. D'un point de vue normatif, le droit du travail ménage une marge de négociation pour les parties au contrat de travail. Ainsi, il revient en général aux parties elles-mêmes de déterminer une partie importante du contenu de leurs relations (voir, *mutatis mutandis*, *Wretlund c. Suède* (déc.), n° 46210/99, 9 mars 2004, affaire relative à la compatibilité avec l'article 8 de la Convention de l'obligation faite à la requérante, employée d'une centrale nucléaire, de se soumettre à des tests de dépistage des drogues ; en ce qui concerne l'action syndicale vue sous l'angle de l'article 11, voir *Gustafsson c. Suède*, 25 avril 1996, § 45, *Recueil* 1996-II, et, *mutatis mutandis*, *Demir et Baykara c. Turquie* [GC], n° 34503/97, §§ 140-146, CEDH 2008, pour le cas particulier des fonctionnaires). Il ressort d'ailleurs des éléments de droit comparé dont dispose la Cour qu'il n'existe pas de consensus européen en la matière. En effet, peu d'États membres ont encadré de manière explicite la question de l'exercice par les employés de leur droit au respect de leur vie privée et de leur correspondance sur leur lieu de travail (paragraphe 52 ci-dessus).

119. À la lumière de ces considérations, la Cour estime que les États contractants doivent se voir accorder une marge d'appréciation étendue pour évaluer la nécessité d'adopter un cadre juridique régissant les conditions dans lesquelles un employeur peut adopter une politique encadrant les communications non professionnelles, électroniques ou autres, de ses employés sur leur lieu de travail.

120. Néanmoins, la latitude dont jouissent les États dans ce domaine ne saurait être illimitée. Les juridictions internes doivent s'assurer que la mise en place par un employeur de mesures de surveillance de la correspondance et des autres communications, quelles qu'en soient l'étendue et la durée, s'accompagne de garanties adéquates et suffisantes contre les abus (voir, *mutatis mutandis*, *Klass et autres c. Allemagne*, 6 septembre 1978, § 50, série A n° 28, et *Roman Zakharov*, précité, §§ 232-234).

121. La Cour est consciente que la situation évolue rapidement dans ce domaine. Toutefois, elle estime que la proportionnalité et les garanties procédurales contre l'arbitraire sont des éléments essentiels. Dans ce contexte, les autorités nationales devraient tenir compte des facteurs suivants.

i) L'employé a-t-il été informé de la possibilité que l'employeur prenne des mesures de surveillance de sa correspondance et de ses autres communications ainsi que de la mise en place de telles mesures ? Si, en pratique, cette information peut être concrètement communiquée au personnel de diverses manières, en fonction des spécificités factuelles de chaque affaire, la Cour estime que, afin que les mesures puissent être jugées conformes aux exigences de l'article 8 de la Convention, l'avertissement

doit en principe être clair quant à la nature de la surveillance et préalable à la mise en place de celle-ci.

ii) Quels ont été l'étendue de la surveillance opérée par l'employeur et le degré d'intrusion dans la vie privée de l'employé ? À cet égard, une distinction doit être faite entre la surveillance du flux des communications et celle de leur contenu. Il faut également prendre en compte les questions de savoir si la surveillance des communications a porté sur leur intégralité ou seulement sur une partie d'entre elles et si elle a ou non été limitée dans le temps ainsi que le nombre de personnes ayant eu accès à ses résultats (voir, en ce sens, *Köpke*, décision précitée). Il en va de même des limites spatiales de la surveillance.

iii) L'employeur a-t-il avancé des motifs légitimes pour justifier la surveillance de ces communications et l'accès à leur contenu même (voir, aux paragraphes 38, 43 et 45 ci-dessus, l'état du droit international et européen en la matière) ? La surveillance du contenu des communications étant de par sa nature une méthode nettement plus invasive, elle requiert des justifications plus sérieuses.

iv) Aurait-il été possible de mettre en place un système de surveillance reposant sur des moyens et des mesures moins intrusifs que l'accès direct au contenu des communications de l'employé ? À cet égard, il convient d'apprécier en fonction des circonstances particulières de chaque espèce le point de savoir si le but poursuivi par l'employeur pouvait être atteint sans que celui-ci n'accède directement et en intégralité au contenu des communications de l'employé.

v) Quelles ont été les conséquences de la surveillance pour l'employé qui en a fait l'objet (voir, *mutatis mutandis*, le critère similaire appliqué pour l'examen de la proportionnalité d'une ingérence dans l'exercice de la liberté d'expression protégée par l'article 10 de la Convention dans *Axel Springer AG c. Allemagne* [GC], n° 39954/08, § 95, 7 février 2012, avec les références citées) ? De quelle manière l'employeur a-t-il utilisé les résultats de la mesure de surveillance, notamment ces résultats ont-ils été utilisés pour atteindre le but déclaré de la mesure (voir, en ce sens, *Köpke*, décision précitée) ?

vi) L'employé s'est-il vu offrir des garanties adéquates, notamment lorsque les mesures de surveillance de l'employeur avaient un caractère intrusif ? Ces 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.

Dans ce contexte, il est opportun de rappeler que pour pouvoir prospérer, les relations de travail doivent se fonder sur la confiance entre les personnes (*Palomo Sánchez et autres*, précité, § 76).

122. Enfin, les autorités internes devraient 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 ci-dessus ainsi que sur la licéité des mesures contestées (*Obst*, précité, § 45 ; et *Köpke*, décision précitée).

123. En l'espèce, la Cour vérifiera la manière dont les juridictions internes saisies par le requérant ont examiné le grief qu'il tirait de l'atteinte portée selon lui par son employeur à son droit au respect de sa vie privée et de sa correspondance dans le cadre des relations de travail.

c) Application en l'espèce des principes généraux

124. La Cour constate que les juridictions nationales ont déterminé qu'entraient en jeu en l'espèce, d'un côté, le droit du requérant au respect de sa vie privée et, de l'autre, le droit de contrôle, y compris les prérogatives disciplinaires, exercé par l'employeur en vue d'assurer le bon fonctionnement de l'entreprise (paragraphes 28 et 30 ci-dessus). Elle estime que, en vertu des obligations positives de l'État au titre de l'article 8 de la Convention, les autorités nationales étaient tenues de mettre en balance ces intérêts divergents.

125. La Cour rappelle que l'objet précis du grief porté devant elle est le manquement allégué des juridictions nationales, saisies dans le cadre d'une procédure de droit du travail, à protéger, conformément à l'article 8 de la Convention, le droit du requérant au respect de sa vie privée et de sa correspondance dans le cadre de sa relation de travail. Tout au long de la procédure, le requérant s'est plaint notamment, tant devant les juridictions internes que devant la Cour, de la surveillance faite par son employeur de ses communications sur les comptes *Yahoo Messenger* en question et de l'utilisation du contenu de ces communications dans le cadre de la procédure disciplinaire dont il a fait l'objet.

126. Sur la question de savoir si l'employeur a divulgué le contenu de ces communications aux collègues du requérant (paragraphe 26 ci-dessus), la Cour observe que cet argument n'est pas suffisamment étayé par les éléments de preuve versés au dossier et que le requérant n'a pas fourni davantage d'éléments lors de l'audience devant la Grande Chambre (paragraphe 91 ci-dessus).

127. Elle estime donc que le grief dont elle est saisie porte sur le licenciement du requérant par suite de la surveillance exercée par l'employeur. Plus précisément, elle doit rechercher en l'espèce si les autorités nationales ont, conformément aux exigences de l'article 8 de la Convention, mis en balance le droit du requérant au respect de sa vie privée et de sa correspondance et les intérêts de l'employeur. Elle a donc pour tâche de déterminer si, à la lumière de l'ensemble de l'affaire, les autorités nationales compétentes ont ménagé un juste équilibre entre les intérêts divergents en jeu lorsqu'elles ont validé les mesures de surveillance imposées au requérant (voir, *mutatis mutandis*, *Palomo Sánchez et autres*, précité, § 62). Elle reconnaît que l'employeur a un intérêt légitime à assurer

le bon fonctionnement de l'entreprise, ce qu'il peut faire en mettant en place des mécanismes lui permettant de vérifier que ses employés accomplissent leurs tâches professionnelles de manière adéquate et avec la célérité requise.

128. À la lumière de ces considérations, elle examinera en premier lieu la façon dont les juridictions nationales ont établi les faits pertinents en l'espèce – tant le tribunal départemental que la cour d'appel ont jugé que le requérant avait reçu un avertissement préalable de la part de son employeur (paragraphe 28 et 30 ci-dessus) – puis elle recherchera si les juridictions nationales ont respecté les exigences de la Convention dans leur examen de l'affaire.

129. À ce stade, la Cour estime utile de rappeler que lorsqu'il s'agit d'établir les faits, sensible à la nature subsidiaire de sa mission, elle ne peut sans de bonnes raisons assumer le rôle de juge du fait de première instance, à moins que cela ne soit rendu inévitable par les circonstances de l'affaire dont elle se trouve saisie (*Mustafa Tunç et Fecire Tunç c. Turquie* [GC], n° 24014/05, § 182, 14 avril 2015). Lorsque des procédures internes ont été menées, elle n'a pas à substituer sa propre version des faits à celle des juridictions nationales, auxquelles il appartient d'établir les faits sur la base des preuves recueillies par elles (voir, parmi d'autres, *Edwards c. Royaume-Uni*, 16 décembre 1992, § 34, série A n° 247-B). Si les constatations de celles-ci ne lient pas la Cour, laquelle demeure libre de se livrer à sa propre évaluation à la lumière de l'ensemble des éléments dont elle dispose, elle ne s'écartera normalement des constatations de fait des juges nationaux que si elle est en possession de données convaincantes à cet effet (*Giuliani et Gaggio c. Italie* [GC], n° 23458/02, § 180, CEDH 2011 (extraits), et *Aydan c. Turquie*, n° 16281/10, § 69, 12 mars 2013).

130. Il ressort des éléments produits devant la Cour que le requérant avait été informé du règlement intérieur de son employeur, qui prohibait l'usage des ressources de l'entreprise à des fins personnelles (paragraphe 12 ci-dessus). Il avait pris connaissance du contenu de ce document et l'avait signé, le 20 décembre 2006 (paragraphe 14 ci-dessus). De plus, l'employeur avait fait circuler parmi tous les employés une note d'information, datée du 26 juin 2007, qui rappelait l'interdiction d'utiliser les ressources de l'entreprise à des fins personnelles et précisait qu'une employée avait été licenciée pour avoir enfreint cette interdiction (paragraphe 15 ci-dessus). Le requérant a pris connaissance de cette note et l'a signée à une date qui n'est pas précisée mais qui se situe entre le 3 et le 13 juillet 2007 (paragraphe 16 ci-dessus). La Cour rappelle enfin que, le 13 juillet 2007, le requérant a été convoqué à deux reprises par son employeur pour donner des explications sur l'usage personnel qu'il avait fait d'internet (paragraphe 18 et 20 ci-dessus). Dans un premier temps, lorsqu'on lui a montré les graphiques présentant son trafic internet et celui de ses collègues, il a affirmé n'avoir utilisé son compte *Yahoo Messenger* qu'à des fins professionnelles (paragraphe 18 et 19 ci-dessus). Puis, lorsque, cinquante minutes plus tard,

on lui a présenté une transcription de 45 pages où figuraient les communications qu'il avait eues avec son frère et sa fiancée, il a informé son employeur qu'il l'estimait responsable de la commission d'une infraction pénale, à savoir la violation du secret de la correspondance (paragraphe 22 ci-dessus).

131. La Cour note que les juridictions nationales ont correctement cerné les intérêts en jeu, en se référant explicitement au droit du requérant au respect de sa vie privée, ainsi que les principes de droit applicables (paragraphe 28 et 30 ci-dessus). En particulier, la cour d'appel s'est référée expressément aux principes de nécessité, de finalité, de transparence, de légitimité, de proportionnalité et de sécurité énoncés dans la directive 95/46/CE, et elle a rappelé que la surveillance de l'utilisation faite d'internet et des communications électroniques sur le lieu de travail était régie par ces principes (paragraphe 30 ci-dessus). Les tribunaux internes ont en outre recherché si la procédure disciplinaire avait été menée dans le respect du principe du contradictoire et si le requérant s'était vu offrir la possibilité de présenter ses arguments.

132. Il reste à vérifier la manière dont les autorités nationales ont pris en compte dans leur raisonnement les critères déjà énoncés ci-dessus (au paragraphe 121) lorsqu'elles ont mis en balance le droit du requérant au respect de sa vie privée et de sa correspondance et le droit de contrôle exercé par l'employeur en vue d'assurer le bon fonctionnement de l'entreprise, y compris les prérogatives disciplinaires correspondantes.

133. En ce qui concerne la question de savoir si le requérant avait reçu un avertissement préalable de la part de son employeur, la Cour rappelle qu'elle a déjà conclu qu'il n'apparaissait pas que l'intéressé eût été informé à l'avance de l'étendue et de la nature de la surveillance opérée par l'entreprise ni de la possibilité que celle-ci ait accès au contenu même de ses communications (paragraphe 78 ci-dessus). Sur la possibilité de la surveillance, elle note que le tribunal départemental s'est borné à constater que « l'attention des employés avait été appelée sur le fait que, peu avant que le requérant ne fasse l'objet d'une sanction disciplinaire, une autre employée avait été licenciée » (paragraphe 28 ci-dessus) et que la cour d'appel a constaté que le requérant avait été averti qu'il ne devait pas utiliser les ressources de l'entreprise à des fins personnelles (paragraphe 30 ci-dessus). Ainsi, les juridictions nationales ont omis de rechercher si le requérant avait été averti préalablement de la possibilité que l'employeur mette en place des mesures de surveillance ainsi que de l'étendue et de la nature de ces mesures. La Cour estime que pour pouvoir être considéré comme préalable, l'avertissement de l'employeur doit être donné avant que celui-ci ne commence son activité de surveillance, *a fortiori* lorsque la surveillance implique également l'accès au contenu des communications des employés. Les normes internationales et européennes vont dans ce sens et exigent que l'information soit communiquée à la personne concernée avant

que celle-ci ne fasse l'objet d'une surveillance (paragraphe 38 et 43 ci-dessus ; voir aussi, pour une perspective de droit comparé, le paragraphe 53 ci-dessus).

134. Quant à l'étendue de la surveillance opérée et du degré d'intrusion dans la vie privée du requérant, la Cour relève que cette question n'a été examinée ni par le tribunal départemental ni par la cour d'appel (paragraphe 28 et 30 ci-dessus), alors qu'il apparaît que l'employeur a enregistré en temps réel l'intégralité des communications passées par le requérant pendant la période de surveillance, qu'il y a eu accès et qu'il en a imprimé le contenu (paragraphe 17 et 21 ci-dessus).

135. Il n'apparaît pas que les juridictions nationales aient suffisamment vérifié la présence de raisons légitimes justifiant la mise en place de la surveillance des communications du requérant. La Cour ne peut que constater que la cour d'appel n'a pas déterminé quel était concrètement dans la présente affaire le but pouvant justifier une surveillance aussi stricte. Il est vrai que cette question avait été évoquée par le tribunal départemental, qui avait mentionné la nécessité d'éviter une atteinte aux systèmes informatiques de l'entreprise, la mise en cause de la responsabilité de l'entreprise en cas d'activité illicite dans l'espace virtuel, ainsi que la révélation de ses secrets commerciaux (paragraphe 28 ci-dessus). Cependant, de l'avis de la Cour, ces exemples ne peuvent être que des indications théoriques puisqu'il n'a été concrètement reproché au requérant d'avoir exposé l'entreprise à aucun de ces risques. Par ailleurs, la cour d'appel ne s'est nullement prononcée sur cette question.

136. Qui plus est, ni le tribunal départemental ni la cour d'appel n'ont examiné de manière suffisante la question de savoir si le but poursuivi par l'employeur aurait pu être atteint par des méthodes moins intrusives que l'accès au contenu même des communications du requérant.

137. De surcroît, ni l'un ni l'autre n'ont examiné la gravité des conséquences de la mesure de surveillance et de la procédure disciplinaire qui s'est ensuivie. À cet égard, la Cour note que le requérant avait fait l'objet de la mesure disciplinaire la plus sévère possible, à savoir un licenciement.

138. Enfin, la Cour relève que les juges nationaux n'ont pas vérifié si, lorsqu'il a convoqué le requérant pour qu'il donne des explications sur l'usage qu'il avait fait des ressources de l'entreprise, et notamment d'internet (paragraphe 18 et 20 ci-dessus), l'employeur n'avait pas déjà eu accès au contenu des communications en cause. Elle observe que les autorités nationales n'ont nullement établi à quel moment de la procédure disciplinaire l'employeur avait eu accès à ce contenu. Elle considère qu'admettre que l'accès au contenu des communications puisse se faire à n'importe quel moment de la procédure disciplinaire va à l'encontre du principe de transparence (voir, en ce sens, la

Recommandation CM/Rec(2015)5 au paragraphe 43 ci-dessus ; pour une perspective de droit comparé, voir le paragraphe 54 ci-dessus).

139. À cet égard, la Cour estime sujette à caution la conclusion de la cour d'appel selon laquelle un juste équilibre entre les intérêts en jeu aurait été ménagé (paragraphe 30 ci-dessus). Ce constat paraît plutôt formel et théorique. En effet, la cour d'appel n'a pas expliqué quelles étaient les raisons concrètes, découlant de la situation spécifique du requérant et de son employeur, qui lui permettraient d'aboutir à ce constat.

140. Dans ces conditions, il apparaît que les juridictions nationales ont manqué, d'une part, à vérifier, en particulier, si le requérant avait été préalablement averti par son employeur de la possibilité que ses communications sur *Yahoo Messenger* soient surveillées et, d'autre part, à tenir compte du fait qu'il n'avait été informé ni de la nature ni de l'étendue de la surveillance dont il avait fait l'objet, ainsi que du degré d'intrusion dans sa vie privée et sa correspondance. De surcroît, elles ont failli à déterminer, premièrement, quelles raisons concrètes avaient justifié la mise en place des mesures de surveillance, deuxièmement, si l'employeur aurait pu faire usage de mesures moins intrusives pour la vie privée et la correspondance du requérant et, troisièmement, si l'accès au contenu des communications avait été possible à son insu (paragraphe 120 et 121 ci-dessus).

141. Eu égard à l'ensemble des considérations qui précèdent et nonobstant la marge d'appréciation de l'État défendeur, la Cour estime que les autorités internes n'ont pas protégé de manière adéquate le droit du requérant au respect de sa vie privée et de sa correspondance et que, dès lors, elles n'ont pas ménagé un juste équilibre entre les intérêts en jeu. Partant, il y a eu violation de l'article 8 de la Convention.

II. SUR L'APPLICATION DE L'ARTICLE 41 DE LA CONVENTION

142. Aux termes de l'article 41 de la Convention,

« Si la Cour déclare qu'il y a eu violation de la Convention ou de ses Protocoles, et si le droit interne de la Haute Partie contractante ne permet d'effacer qu'imparfaitement les conséquences de cette violation, la Cour accorde à la partie lésée, s'il y a lieu, une satisfaction équitable. »

A. Dommage

1. Dommage matériel

143. Devant la chambre, le requérant réclamait 59 976,12 euros (EUR) au titre du préjudice matériel qu'il estimait avoir subi. Il expliquait que cette somme représentait la valeur actualisée des salaires auxquels il aurait eu droit s'il n'avait pas été licencié. Au cours de l'audience devant la Grande

Chambre, les représentants du requérant ont indiqué qu'ils maintenaient leur demande de satisfaction équitable.

144. Dans ses observations devant la chambre, le Gouvernement avait indiqué qu'il s'opposait à l'octroi d'une quelconque somme au titre du préjudice matériel prétendument subi. À son avis, la somme réclamée relevait de la spéculation et il n'y avait pas de lien entre le licenciement du requérant et le préjudice allégué.

145. La Cour rappelle qu'elle a conclu à la violation de l'article 8 de la Convention, les juridictions nationales ayant manqué à établir les faits pertinents et à mettre en balance de manière adéquate le droit du requérant au respect de sa vie privée et de sa correspondance et les intérêts de l'employeur. Elle n'aperçoit pas de lien de causalité entre la violation constatée et le dommage matériel allégué et, dès lors, elle rejette cette demande.

2. Dommage moral

146. Devant la chambre, le requérant réclamait également 200 000 EUR au titre du préjudice moral qu'il estimait avoir subi du fait de son licenciement. Il indiquait qu'en raison du motif disciplinaire de ce licenciement, il n'avait pas pu retrouver un autre emploi, que son niveau de vie s'était ainsi dégradé, qu'il avait perdu son statut social, et qu'en conséquence, sa fiancée avait décidé, en 2010, de mettre fin à leur relation.

147. Le Gouvernement répondait à cela qu'un éventuel constat de violation pouvait constituer en lui-même une satisfaction équitable suffisante. En tout état de cause, il estimait que la somme réclamée par le requérant était exorbitante par rapport à la jurisprudence de la Cour en la matière.

148. La Cour estime que le constat d'une violation constitue une satisfaction équitable suffisante pour tout dommage moral pouvant avoir été subi par le requérant.

B. Frais et dépens

149. Devant la chambre, le requérant réclamait également 3 310 lei roumains (RON) (soit environ 750 EUR), au titre des frais et dépens engagés devant les juridictions internes, ainsi que 500 RON (soit environ 115 EUR), pour les honoraires de l'avocat qui l'avait représenté devant les tribunaux internes. Il demandait également 500 EUR pour les honoraires des avocats qui l'avaient représenté devant la Cour. Il avait fourni à l'appui de sa demande :

- les copies du contrat d'assistance juridique et de la quittance du paiement de la somme de 500 RON, correspondant aux honoraires de l'avocat l'ayant représenté devant les tribunaux internes ;

- des documents prouvant qu'il avait payé à son employeur les sommes de 2 700 RON et 610,30 RON au titre des frais et dépens ;
- la copie de la quittance du paiement de la somme de 2 218,64 RON, correspondant aux honoraires de l'un des avocats l'ayant représenté devant la Cour.

Le requérant n'a pas demandé le remboursement des frais engagés dans le cadre de la procédure menée devant la Grande Chambre.

150. Dans ses observations devant la chambre, le Gouvernement avait prié la Cour de n'allouer au requérant que les sommes nécessaires et correspondant à des demandes dûment étayées. À cet égard, il indiquait que le requérant n'avait pas prouvé avoir payé 500 EUR d'honoraires aux avocats qui l'avaient représenté devant la Cour, et que la quittance de paiement d'une somme de 500 RON d'honoraires à l'avocat qui l'avait représenté devant les juridictions nationales n'était pas accompagnée du justificatif des heures de travail.

151. Selon la jurisprudence de la Cour, un requérant ne peut obtenir le remboursement de ses frais et dépens que dans la mesure où se trouvent établis leur réalité, leur nécessité et le caractère raisonnable de leur taux (voir, en ce sens, *Paroisse gréco-catholique Lupeni et autres c. Roumanie* [GC], n° 76943/11, § 187, CEDH 2016 (extraits)). En l'espèce, compte tenu des documents dont elle dispose et de sa jurisprudence, la Cour estime raisonnable la somme de 1 365 EUR tous frais confondus et l'accorde au requérant.

C. Intérêts moratoires

152. La Cour juge approprié de calquer le taux des intérêts moratoires sur le taux d'intérêt de la facilité de prêt marginal de la Banque centrale européenne majoré de trois points de pourcentage.

PAR CES MOTIFS, LA COUR

1. *Dit*, par onze voix contre six, qu'il y a eu violation de l'article 8 de la Convention ;
2. *Dit*, par seize voix contre une, que le constat d'une violation constitue une satisfaction équitable suffisante pour le dommage moral subi par le requérant ;
3. *Dit*, par quatorze voix contre trois,
 - a) que l'État défendeur doit verser au requérant, dans les trois mois, la somme de 1 365 EUR (mille trois cent soixante-cinq euros), à convertir

dans la monnaie de l'État défendeur, au taux applicable à la date du règlement, plus tout montant pouvant être dû par le requérant à titre d'impôt sur cette somme, pour frais et dépens ;

b) qu'à compter de l'expiration dudit délai et jusqu'au versement, ce montant sera à majorer d'un intérêt simple à un taux égal à celui de la facilité de prêt marginal de la Banque centrale européenne applicable pendant cette période, augmenté de trois points de pourcentage ;

4. Rejette, à l'unanimité, la demande de satisfaction équitable pour le surplus.

Fait en français et en anglais, puis prononcé en audience publique au Palais des droits de l'homme, à Strasbourg, le 5 septembre 2017.

Søren Prebensen
Adjoint au greffier

Guido Raimondi
Président

Au présent arrêt se trouve joint, conformément aux articles 45 § 2 de la Convention et 74 § 2 du règlement, l'exposé des opinions séparées suivantes :

- opinion partiellement dissidente de la juge Karakaş ;
- opinion dissidente commune aux juges Raimondi, Dedov, Kjølbro, Mits, Mourou-Vikström et Eicke.

G.R.
S.C.P.

OPINION PARTIELLEMENT DISSIDENTE DE LA JUGE KARAKAŞ

Je souscris entièrement à la conclusion de violation de l'article 8 de la Convention rendue par la majorité.

En revanche, je ne partage pas l'opinion de la majorité lorsqu'elle estime qu'un constat de violation constitue une satisfaction équitable suffisante pour le dommage moral subi par le requérant.

Il va de soi que la Cour décide au titre de l'article 41 d'allouer un certain montant pour dommage moral si elle considère qu'« il y a lieu » d'accorder une réparation. Jouissant d'une grande latitude pour déterminer dans quels cas il y a lieu d'octroyer des dommages et intérêts aux requérants, la Cour conclut parfois que le constat de violation représente une satisfaction équitable suffisante et que l'octroi d'une indemnité pécuniaire ne s'impose pas (voir, parmi beaucoup d'autres, *Nikolova c. Bulgarie* [GC], n° 31195/96, § 76, CEDH 1999-II, *Vinter et autres c. Royaume-Uni* [GC], n°s 66069/09 et 2 autres, CEDH 2013 (extraits), et *Murray c. Pays-Bas* [GC], n° 10511/10, CEDH 2016). Pour arriver à cette conclusion, elle prend en compte l'ensemble des faits de la cause, notamment la nature des violations qu'elle a constatées ainsi que les éventuelles particularités du contexte dans lequel l'affaire s'inscrit (voir, par exemple, *Vinter*, précité, et l'opinion en partie dissidente commune aux juges Spielmann, Sajó, Karakaş et Pinto de Albuquerque jointe à l'arrêt *Murray*, précité). Si les circonstances de l'affaire le justifient, comme dans l'affaire *McCann et autres c. Royaume-Uni* (27 septembre 1995, § 219, série A n° 324), dans laquelle la Cour a refusé d'accorder la moindre indemnité pour préjudice moral eu égard au fait que les trois terroristes présumés qui avaient été abattus avaient l'intention de poser une bombe à Gibraltar, ou si la nature de la violation constatée le justifie, comme dans l'affaire *Tarakhel c. Suisse* ([GC], n° 29217/12, CEDH 2014 (extraits)), elle décide que le constat de violation fournit en soi une satisfaction équitable suffisante pour un éventuel préjudice moral. Autrement dit, c'est uniquement dans des cas très exceptionnels que la Cour décide de ne pas octroyer de somme au titre du dommage moral.

Il peut également y avoir des cas où la Cour décide d'allouer une somme inférieure à celle accordée dans d'autres affaires relevant de l'article concerné, toujours en considération des particularités du contexte. Par exemple, dans l'affaire *A. et autres c. Royaume-Uni* ([GC], n° 3455/05, CEDH 2009), dans le contexte du terrorisme, la Cour a expliqué dans une longue motivation (§ 252 ; voir aussi *Del Río Prada c. Espagne* [GC], n° 42750/09, § 145, CEDH 2013) les raisons qui justifiaient l'octroi d'une somme nettement inférieure à celle qu'elle avait accordée dans d'autres affaires de détention irrégulière.

En l'espèce, les juridictions nationales n'ont pas protégé de manière adéquate le droit du requérant au respect de sa vie privée et de sa correspondance ; celui-ci a durement pâti de la procédure disciplinaire dirigée contre lui puisqu'il a été licencié.

Cette violation de l'article 8 a certainement causé un dommage moral au requérant, qui ne peut pas se satisfaire du seul constat de son préjudice. C'est la raison pour laquelle j'étais favorable à l'octroi d'une somme, même minimale, au titre de la satisfaction équitable pour le préjudice moral subi par le requérant.

OPINION DISSIDENTE COMMUNE AUX JUGES
RAIMONDI, DEDOV, KJØLBRO, MITS,
MOUROU–VIKSTRÖM ET EICKE

(Traduction)

Introduction

1. Nous partageons, certains d'entre nous avec quelque hésitation, l'avis de la majorité selon lequel, même dans un contexte où, compte tenu des faits portés à la connaissance de la Cour, il est difficile de concevoir comment le requérant aurait pu avoir une « attente raisonnable en matière de respect de la vie privée » (voir plus bas), l'article 8 trouve à s'appliquer dans les circonstances de la cause (paragraphe 69 à 81 de l'arrêt). Une fois posée l'applicabilité de l'article 8, nous convenons également que le grief du requérant doit être analysé sous l'angle des obligations positives de l'État (paragraphe 111 de l'arrêt). Sous réserve de ce qui suit, nous souscrivons également aux principes généraux applicables à l'appréciation de l'obligation positive qui incombe à l'État, tels que décrits aux paragraphes 113 à 122 de l'arrêt.

2. Cependant, pour les raisons qui seront exposées plus bas, et avec tout le respect que nous devons à la majorité, nous exprimons notre désaccord avec elle sur l'approche qui doit être déployée en relation avec l'obligation positive de l'État en l'espèce ainsi que sur sa conclusion finale selon laquelle les « autorités internes », expression par laquelle la majorité désigne uniquement les juridictions du travail, « n'ont pas protégé de manière adéquate le droit du requérant au respect de sa vie privée et de sa correspondance et que, dès lors, elles n'ont pas ménagé un juste équilibre entre les intérêts en jeu » (paragraphe 141 de l'arrêt).

Principe

3. Étant donné que nul ne conteste que la présente requête doit être analysée sous l'angle de l'obligation positive qui incombe à l'État au titre de l'article 8, le point de départ à retenir est à rechercher dans la jurisprudence de la Cour qui définit la teneur et la portée de la notion d'« obligations positives » au regard de cet article. La Grande Chambre a synthétisé les principes pertinents en dernier lieu dans l'arrêt *Söderman c. Suède* ([GC], n° 5786/08 §§ 78-85, CEDH 2013), qui traitait de l'obligation positive de protéger l'intégrité physique et morale de la requérante face à autrui. La Cour y a clairement exposé les points suivants :

a) si l'article 8 a essentiellement pour objet de prémunir l'individu contre les ingérences arbitraires des pouvoirs publics, il ne se contente

pas de commander à l'État de s'abstenir de pareilles ingérences : à cet engagement plutôt négatif s'ajoutent des obligations positives inhérentes à un respect effectif de la vie privée ou familiale. Elles peuvent impliquer l'adoption de mesures visant au respect de la vie privée jusque dans les relations des individus entre eux (voir, parmi d'autres, *Airey c. Irlande*, 9 octobre 1979, § 32, série A n° 32) (*Söderman*, précité, § 78) ;

b) le choix des mesures propres à garantir l'observation de l'article 8 dans les rapports interindividuels relève en principe de la marge d'appréciation des États contractants, que les obligations à la charge de l'État soient positives ou négatives. Il existe en effet différentes manières d'assurer le respect de la vie privée, et la nature de l'obligation de l'État dépend de l'aspect de la vie privée qui se trouve en cause (voir, par exemple, *Von Hannover c. Allemagne (n° 2)* [GC], n°s 40660/08 et 60641/08, § 104, CEDH 2012, *Odièvre c. France* [GC], n° 42326/98, § 46, CEDH 2003-III, *Evans c. Royaume-Uni* [GC], n° 6339/05, § 77, CEDH 2007-I, et *Mosley c. Royaume-Uni*, n° 48009/08, § 109, 10 mai 2011) (*Söderman*, précité, § 79) ; et

c) pour ce qui est des actes interindividuels de moindre gravité susceptibles de porter atteinte à l'intégrité morale, l'obligation qui incombe à l'État, au titre de l'article 8, de mettre en place et d'appliquer en pratique un cadre juridique adapté offrant une protection n'implique pas toujours l'adoption de dispositions pénales efficaces visant les différents actes pouvant être en cause. Le cadre juridique peut aussi consister en des recours civils aptes à fournir une protection suffisante (voir, *mutatis mutandis*, *X et Y c. Pays-Bas*, 26 mars 1985, §§ 24 et 27, série A n° 91, et *K.U. c. Finlande*, n° 2872/02, § 47, CEDH 2008). La Cour observe, par exemple, que dans certaines affaires précédentes relatives à la protection de l'image d'une personne contre des abus de la part d'autrui, les recours existants dans les États membres étaient d'ordre civil, parfois combinés à des voies procédurales telles que le prononcé d'une interdiction (voir, parmi d'autres, *Von Hannover*, précité, *Reklos et Davourlis c. Grèce*, n° 1234/05, 15 janvier 2009, et *Schüssel c. Autriche* (déc.), n° 42409/98, 21 février 2002) (*Söderman*, précité, § 85).

4. Les faits de la cause, comme l'admet, du moins implicitement, la majorité (paragraphe 80 de l'arrêt), se situent naturellement à mille lieues de la gravité des actes considérés dans l'arrêt *Söderman*. En effet, dans cette affaire, la Cour avait eu à se pencher sur des allégations de violation de l'intégrité physique et morale d'une personne par une autre personne.

5. Néanmoins, même dans ce contexte, il est clair, en premier lieu, que le choix des mesures conçues pour garantir le respect de la vie privée protégé par l'article 8, y compris dans la sphère des relations interpersonnelles, appartient au premier chef aux États contractants, et que c'est un choix pour lequel ceux-ci bénéficient d'une marge d'appréciation étendue (paragraphe 119 de l'arrêt ; cette marge se restreint lorsque,

contrairement à la situation en l'espèce, un aspect particulièrement important de l'existence ou de l'identité d'un individu se trouve en jeu, ou que les activités en cause concernent un aspect des plus intimes de la vie privée). Cette conclusion est corroborée par le fait qu'il n'existe pas de consensus européen en la matière et que seulement six des 34 États membres du Conseil de l'Europe étudiés encadrent explicitement la question de l'exercice de la vie privée sur le lieu de travail (paragraphe 52 et 118 de l'arrêt). En second lieu, les « mesures » adoptées par l'État au titre de l'article 8 devraient en principe revêtir la forme d'un « cadre juridique » adéquat offrant une protection à la victime. L'article 8 n'implique pas toujours l'adoption d'une disposition pénale efficace visant l'acte spécifique qui est en cause. Le cadre juridique peut aussi consister en des recours civils aptes à fournir une protection suffisante.

6. Ces considérations s'appliquent naturellement *mutatis mutandis* à la présente espèce où, comme le relève la majorité, la Cour est au mieux appelée à se prononcer sur la protection d'un degré élémentaire ou minimum de vie privée et de correspondance sur le lieu de travail contre une atteinte de la part d'un employeur de droit privé.

Le périmètre de l'examen de la Cour

7. Ayant cité quelques-uns des principes énoncés ci-dessus, la majorité a, au paragraphe 123, réduit à notre avis de manière injustifiable le périmètre de son examen à « la manière dont les juridictions internes saisies par le requérant ont examiné le grief qu'il tirait de l'atteinte portée selon lui par son employeur à son droit au respect de sa vie privée et de sa correspondance dans le cadre des relations de travail ».

8. Bien que reconnaissant que « des mesures protectrices peuvent être prévues tant par le droit du travail que par le droit civil et le droit pénal » (paragraphe 116 de l'arrêt), la majorité opte pour l'esquive et évite en réalité de répondre à la véritable question qui se pose : la Haute Partie contractante a-t-elle mis en place et appliqué un « cadre juridique » adapté offrant au moins des recours civils aptes à fournir au requérant une protection suffisante ?

9. Comme l'indique le gouvernement défendeur et comme l'admet la majorité, le « cadre juridique » pertinent en Roumanie se composait non seulement des juridictions du travail que le requérant avait saisies de son grief mais aussi, entre autres, des éléments suivants :

a) l'infraction pénale de « violation du secret de la correspondance » prévue par l'article 195 du code pénal (paragraphe 33 de l'arrêt) ; incidemment, il s'agit d'un recours que le requérant avait engagé en déposant une plainte pénale mais que, le parquet ayant rendu une décision de non-lieu, il n'a pas exercé jusqu'au bout faute d'avoir

contesté cette décision devant les juridictions internes (paragraphe 31 de l'arrêt) ;

b) les dispositions de la loi n° 677/2001 « relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation des données à caractère personnel » (paragraphe 36 de l'arrêt) laquelle, en prévision de l'adhésion de la Roumanie à l'Union européenne, reprend certaines dispositions de la Directive 95/46/CE du 24 octobre 1995 du Parlement européen et du Conseil de l'Union européenne relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données. Dans son article 18, cette loi prévoit expressément un droit i) d'adresser une plainte à l'autorité de surveillance et, à titre subsidiaire ou dans un deuxième temps, ii) de saisir les tribunaux compétents en vue de la protection des droits relatifs aux données à caractère personnel garantis par cette loi, y compris le droit d'obtenir réparation de son préjudice ; et

c) les dispositions du code civil (articles 998 et 999 ; paragraphe 34 de l'arrêt) permettant d'introduire une action en responsabilité civile délictuelle dans le but d'obtenir réparation du dommage subi, que celui-ci ait été causé délibérément ou par négligence.

10. Hormis la plainte pénale qui n'a pas eu de suite, le requérant n'a jamais exercé de voies de recours internes. Il s'est contenté de saisir les juridictions du travail pour contester non pas principalement l'atteinte par son employeur à sa vie privée/sa correspondance mais son licenciement. Comme le note la majorité au paragraphe 24 de l'arrêt :

« Il priait le tribunal, premièrement, d'annuler cette décision [de licenciement], deuxièmement, d'ordonner à son employeur de lui verser les sommes auxquelles il estimait avoir droit au titre de son salaire et d'autres créances et de le réintégrer à son poste et, troisièmement, de condamner l'employeur à lui payer des dommages-intérêts d'un montant de 100 000 lei roumains (environ 30 000 euros) au titre du préjudice moral qu'il estimait avoir subi du fait des modalités de son licenciement, et à lui rembourser ses frais et dépens. »

11. Ce n'est que dans le contexte de cette procédure de contestation de son licenciement que, se fondant sur l'arrêt *Copland c. Royaume-Uni* (n° 62617/00, §§ 43-44, CEDH 2007-I), il a avancé l'argument selon lequel la décision de le licencier avait été illégale et qu'en surveillant ses communications et en accédant à leur contenu, son employeur avait enfreint le droit pénal.

12. Le fait que le requérant s'est attaché principalement, si ce n'est exclusivement, à la légalité de son licenciement plutôt qu'à l'atteinte par son employeur à son droit au respect de la vie privée et de la correspondance transparait également dans la manière dont il a présenté son affaire devant la Cour. Comme le relève l'arrêt au paragraphe 55, le requérant soutient que « la mesure de licenciement prise par son employeur reposait sur une

violation à son égard du droit au respect de la vie privée et de la correspondance et que, dès lors qu'elles n'ont pas annulé cette mesure, les juridictions internes ont manqué à leur obligation de protéger ce droit. »

13. Par conséquent, on ne peut s'empêcher de noter (ne serait-ce qu'en passant) que, si le gouvernement défendeur avait soulevé ce point à titre d'exception préliminaire, se serait posée la question de savoir si, en saisissant les juridictions du travail sur la base qu'il avait choisie, le requérant avait bien épuisé les recours internes qui étaient « à la fois relatifs à la violation incriminée, disponibles et adéquats » (*Aquilina c. Malte* [GC], n° 25642/94, § 39, CEDH 1999-III). Après tout, la Cour n'a pas en sa possession d'élément de nature à laisser penser que l'une des trois voies de recours énumérées ci-dessus et, en particulier, une plainte auprès de l'autorité spécialisée dans la supervision de la protection des données et/ou une action en réparation fondée sur les dispositions de la loi n° 677/2001 devant les juridictions compétentes, étaient « vouées à l'échec » (*Davydov et autres c. Russie*, n° 75947/11, § 233, 30 mai 2017).

14. Nos doutes à propos de l'efficacité des juridictions du travail dans ce contexte (et du bien-fondé de la décision de la Cour de restreindre son examen à l'adéquation de l'analyse qu'elles ont effectuée) sont encore exacerbés par le constat que, dans le droit fil de la jurisprudence de la Cour relative à l'article 6 de la Convention, le fait que les actions de l'employeur aient ou non été illégales ne pouvait pas en lui-même compromettre la validité de la procédure disciplinaire tenue en l'espèce. Après tout, comme l'a confirmé la Cour en dernier lieu dans l'arrêt *Vukota-Bojić c. Suisse*, n° 61838/10, §§ 94-95, 18 octobre 2016 :

« (...) pour déterminer si l'utilisation comme preuves d'informations obtenues au mépris de l'article 8 a privé le procès dans son ensemble du caractère équitable voulu par l'article 6, il faut prendre en compte toutes les circonstances de la cause et se demander en particulier si les droits de la défense ont été respectés et quelles sont la qualité et l'importance des éléments en question (comparer, entre autres, avec *Khan*, précité, §§ 35-40 ; *P.G. et J.H. c. Royaume-Uni*, précité, §§ 77-79, et *Bykov c. Russie* [GC], n° 4378/02, §§ 94-98, 10 mars 2009, dans lesquels la Cour n'a pas constaté de violation de l'article 6).

Il y a lieu de se demander en particulier si le requérant a eu la possibilité de contester l'authenticité des preuves et de s'opposer à leur utilisation. Il faut également prendre en compte la qualité des preuves et notamment vérifier si les circonstances dans lesquelles elles ont été obtenues jettent le doute sur leur crédibilité ou leur exactitude. Enfin, la Cour attachera de l'importance au point de savoir si l'élément de preuve en question a exercé une influence décisive sur l'issue de l'action (comparer, en particulier, avec *Khan*, précité, §§ 35 et 37). »

15. En tout état de cause, les autres voies de recours internes susmentionnées, dont certaines sont à l'évidence mieux adaptées à la protection de la vie privée et de la correspondance d'un individu sur son lieu de travail chez un employeur privé, auraient assurément permis de déterminer si le « cadre juridique » mis en place par la Roumanie était de

nature à offrir une protection « adéquate » au requérant face à une atteinte illicite à son droit au respect de la vie privée/de la correspondance garanti par l'article 8 par un autre particulier (en l'occurrence, son employeur).

16. En s'abstenant de les inclure dans son analyse ou en les y incluant à un degré insuffisant, la majorité a laissé de côté des facteurs importants concernant la question posée en l'espèce et n'a pas accordé le poids qu'elle aurait méritée à l'ample marge d'appréciation qui est reconnue aux Hautes Parties contractantes lorsqu'il s'agit de définir les mesures à prendre et les voies de recours à offrir pour honorer l'obligation positive qui leur incombe, en vertu de l'article 8, de mettre en place un « cadre juridique » adéquat. Faute d'éléments donnant à penser que les voies de recours internes n'étaient pas, chacune ou globalement, suffisamment disponibles ou effectives pour offrir la protection requise par l'article 8, il nous semble que la Cour ne dispose d'aucune base qui lui permette de dire qu'il y a eu violation de l'article 8 dans les circonstances de l'espèce.

17. Pour dire un dernier mot sur la question du périmètre adéquat pour l'examen de la Cour, nous tenons à préciser que nous souhaitons sincèrement que l'arrêt adopté par la majorité ne soit pas lu comme consacrant une obligation générale au titre de la Convention par laquelle, lorsque le cadre juridique interne offre des recours plus appropriés (tels que ceux qui doivent être mis en place en application de la législation pertinente de l'Union européenne sur la protection des données), les juridictions du travail nationales qui auront à connaître d'affaires semblables à celle du requérant seront tenues de dupliquer les fonctions de la voie de recours spécialisée qui serait plus appropriée.

L'analyse effectuée par les juridictions du travail internes

18. Toutefois, même à supposer que, contrairement à ce qui est exposé ci-dessus, le choix de la majorité de restreindre son examen à l'analyse effectuée par les juridictions du travail internes soit la bonne approche, nous ne pensons pas non plus que ladite analyse était déficiente au point de conduire à un constat de violation de l'article 8.

19. Il ressort des jugements prononcés par le tribunal départemental et par la cour d'appel de Bucarest que ces deux juridictions nationales ont pris en considération le règlement intérieur de l'employeur, lequel interdisait l'utilisation des ressources de l'entreprise à des fins personnelles (paragraphe 12, 28 et 30 de l'arrêt). Nous observons également que le requérant avait été informé du règlement intérieur de l'employeur et en avait signé un exemplaire, après avoir pris connaissance de son contenu, le 20 décembre 2006 (paragraphe 14 de l'arrêt). Les tribunaux internes ont interprété les dispositions de ce texte comme sous-entendant qu'il était possible que soient mises en place des mesures de surveillance des communications, éventualité qui était de nature à réduire de manière

significative la probabilité que le requérant pût raisonnablement s'attendre à ce que le caractère privé de sa correspondance fût respecté (voir, *a contrario*, *Halford c. Royaume-Uni*, 25 juin 1997, § 45, *Recueil des arrêts et décisions* 1997-III, et *Copland*, précité, § 42). Nous considérons donc que la question de l'avertissement préalable aurait dû être examinée dans ce contexte.

20. Dans ces conditions, il est clair, au vu des éléments dont dispose la Cour, que les juridictions nationales ont effectivement examiné cette question. Tant le tribunal départemental que la cour d'appel ont accordé un poids certain à la note d'information que le requérant avait signée, et il ressort de leurs décisions qu'un exemplaire signé de cette note avait été produit devant elles (paragraphe 28 et 30 de l'arrêt). Le tribunal départemental a notamment observé que l'employeur avait prévenu ses employés que leurs activités, y compris l'usage qu'ils faisaient des ordinateurs, étaient surveillées, et a également relevé que le requérant lui-même avait pris connaissance de la note d'information (paragraphe 28 de l'arrêt). La cour d'appel a confirmé que « l'utilisation [des ressources de l'entreprise] à des fins personnelles p[ouvai]t être refusée (...) en application des dispositions du règlement intérieur » dont les employés avaient été dûment informés (paragraphe 30 de l'arrêt). Ainsi, les juridictions nationales ont jugé, sur la base des documents en leur possession, que le requérant avait été suffisamment averti de ce que ses activités, y compris l'usage qu'il faisait de l'ordinateur mis à disposition par son employeur, pouvaient être surveillées. Nous ne voyons aucune raison de nous écarter de leurs décisions et considérons que le requérant pouvait raisonnablement s'attendre à ce que ses activités fussent surveillées.

21. Nous notons ensuite que les autorités nationales ont procédé à une mise en balance circonstanciée des intérêts en jeu : elles ont tenu compte, d'un côté, du droit du requérant au respect de sa vie privée et, de l'autre, du droit de l'employeur à exercer une surveillance, ainsi que les pouvoirs disciplinaires dont elle s'accompagne, en vue d'assurer le bon fonctionnement de l'entreprise (paragraphe 28 et 30 de l'arrêt ; voir également, *mutatis mutandis*, *Obst c. Allemagne*, n° 425/03, § 49, 23 septembre 2010 et *Fernández Martínez c. Espagne* [GC], n° 56030/07, § 151, CEDH 2014 (extraits)). La cour d'appel, en particulier, citant les dispositions de la Directive 95/46/CE, a noté qu'il y avait en l'espèce un conflit entre « le droit de surveillance de l'employeur et le droit des employés à la protection de leur vie privée » (paragraphe 30 de l'arrêt).

22. Nous relevons également que, se fondant sur les éléments de preuve en leur possession, les juridictions nationales ont estimé que le but légitime que poursuivait l'employeur lorsqu'il a mis en place l'opération de surveillance des communications du requérant était d'exercer « le droit et l'obligation d'assurer le fonctionnement de l'entreprise » (voir la décision de la cour d'appel citée au paragraphe 30 de l'arrêt). Si les juridictions

internes ont accordé plus de poids au droit pour l'employeur d'assurer le bon fonctionnement de l'entreprise et de surveiller la façon dont les employés accomplissaient leurs tâches dans le cadre de leur relation de travail qu'au droit du requérant au respect de sa vie privée et de sa correspondance, nous considérons qu'il n'est pas déraisonnable pour un employeur de vouloir vérifier que ses employés accomplissent leurs tâches professionnelles lorsqu'ils font usage sur leur lieu de travail et pendant leurs heures de travail du matériel qu'il met à leur disposition. La cour d'appel a estimé que la surveillance des communications du requérant était le seul moyen pour l'employeur d'atteindre ce but légitime, ce qui l'a amenée à conclure qu'un juste équilibre avait été ménagé entre la nécessité de protéger la vie privée du requérant et le droit pour l'employeur de superviser le fonctionnement de son entreprise (paragraphe 30 de l'arrêt).

23. À notre avis, le choix des autorités nationales de privilégier les intérêts de l'employeur par rapport à ceux de l'employé n'est pas en lui-même de nature à soulever un problème au regard de la Convention (voir, *mutatis mutandis*, *Obst*, précité, § 49). Nous souhaitons ici rappeler que lorsqu'elles doivent ménager un équilibre entre plusieurs intérêts privés concurrents, les autorités jouissent d'une certaine latitude (*Hämäläinen c. Finlande* [GC], n° 37359/09, § 67, CEDH 2014, *in fine*, avec les références citées). En l'espèce, à notre avis, les juridictions internes ont donc agi dans le cadre de la marge d'appréciation qui était la leur en Roumanie.

24. Nous relevons par ailleurs que la mesure de surveillance dont le requérant a fait l'objet a été limitée dans le temps et qu'il ressort des éléments produits devant la Cour que l'employeur n'a surveillé que les communications électroniques et le trafic Internet du requérant. Ce dernier n'a d'ailleurs pas allégué qu'un autre aspect de sa vie privée, telle qu'exercée dans le contexte professionnel, ait fait l'objet de mesures de surveillance de la part de son employeur. De surcroît, il ressort des éléments dont dispose la Cour que les résultats de l'opération de surveillance ont été utilisés aux seules fins de la procédure disciplinaire engagée à l'encontre du requérant et que n'ont eu accès au contenu des communications de l'intéressé que les personnes ayant participé à cette procédure (pour une approche similaire, voir *Köpke c. Allemagne* (déc.), n° 420/07, 5 octobre 2010). À cet égard, il y a lieu d'observer que la majorité convient que le requérant n'a pas étayé ses allégations selon lesquelles le contenu en question aurait été divulgué à d'autres collègues (paragraphe 126 de l'arrêt).

25. Enfin, nous observons que dans leur examen de l'affaire, les autorités nationales ont pris en compte l'attitude dont le requérant avait fait preuve pendant son activité professionnelle en général, et pendant la procédure disciplinaire dont il avait fait l'objet en particulier. Ainsi, le tribunal départemental a jugé que le requérant s'était rendu coupable d'une faute disciplinaire en méconnaissant le règlement intérieur de son

employeur, qui prohibait l'usage des ordinateurs à des fins personnelles (paragraphe 28 de l'arrêt). Dans leur analyse, les autorités internes ont accordé beaucoup de poids à l'attitude qui avait été celle du requérant pendant la procédure disciplinaire, au cours de laquelle il avait nié avoir utilisé les ressources de son employeur à des fins personnelles et avait affirmé n'en avoir fait usage qu'à des fins professionnelles, ce qui était faux (paragraphe 28 et 30 de l'arrêt). Elles étaient clairement en droit de le faire. Cela a été confirmé lorsque le requérant a avancé devant la Cour que, bien qu'il sût qu'il était interdit d'utiliser son ordinateur professionnel à des fins privées, seul le fait de se savoir surveillé par son employeur l'avait dissuadé d'utiliser à des fins privées l'ordinateur mis à sa disposition sur son lieu de travail ; il n'a pas nié qu'il avait été informé de cette surveillance mais s'est dit incapable de se souvenir de la date à laquelle il avait reçu la note d'information l'en avisant.

26. Après tout, comme la majorité le souligne également (paragraphe 121 de l'arrêt), pour pouvoir prospérer, les relations de travail doivent se fonder sur la confiance entre les personnes (*Palomo Sánchez et autres c. Espagne* [GC], n^{os} 28955/06 et 3 autres, § 76, CEDH 2011). Dès lors, nous estimons que vu leur marge d'appréciation les juridictions internes (du travail) étaient en droit de tenir compte, dans leur mise en balance des intérêts en jeu, de l'attitude qui avait été adoptée par le requérant, lequel avait rompu le lien de confiance avec son employeur.

27. Eu égard à l'ensemble des considérations qui précèdent et contrairement à la majorité, nous concluons qu'il n'y a pas eu de défaut de protection du droit du requérant au respect de sa vie privée et de sa correspondance et que, partant, il n'y a pas eu violation de l'article 8 de la Convention.