5. Noms de domaine

93. Enregistrement prioritaire. Au cours de la période sous revue, l'on relèvera l'arrêt de la Cour de justice dans l'affaire *Pie Optiek*, dans lequel il a été jugé qu'un contrat de services comportant un aspect de licence de droits de marque ne peut être qualifié de contrat de licence, car il n'emporte aucune concession d'un droit propre d'exploitation commerciale des fonctions de la marque au bénéfice du « licencié ». Dès lors, un tel contrat ne permet pas à la partie prestataire de services (bénéficiant de la « licence » de marque) d'être éligible au régime d'enregistrement prioritaire des noms de domaine.eu tel qu'organisé par le règlement n° 874/2004 établissant les règles de politique d'intérêt général relatives à la mise en œuvre et aux fonctions du domaine de premier niveau.eu et les principes applicables en matière d'enregistrement[392].

94. Application des règles relatives à la publicité. Enfin, l'on relèvera encore un arrêt de la Cour de justice dans lequel est abordée la possible qualification de l'enregistrement d'un nom de domaine en tant que « publicité » au sens de la réglementation sur les pratiques commerciales[393].

III. LIBERTÉS ET SOCIÉTÉ DE L'INFORMATION

A. Vie privée et protection des données à caractère personnel

1. Juridictions judiciaires[394] (Christine Burnet, Maxime Piron[395]) *et constitutionnelle* (Bénédicte Losdyck, Odile Vanreck[396] et Jean-Marc Van Gyseghem)

95. Introduction. Nous analysons dans cette partie les décisions rendues entre 2012 et 2014 par les juridictions judiciaires et la Cour constitutionnelle en matière de vie privée et de protection des données à caractère personnel en relation avec les nouvelles technologies. Nous avons opéré, pour des raisons d'impératifs éditoriaux, une sélection des décisions qui nous paraissent les plus pertinentes sans aucune volonté d'exhaustivité. Par ailleurs, de nombreuses décisions rendues en matière de protection de la vie privée et de données à caractère personnel l'ont été dans des matières qui font l'objet d'autres contributions de la présente chronique. Elles ne sont donc pas reprises ici.

a. Droit au respect de la vie privée

96. Vie privée et devoir d'information. Dans un arrêt rendu le 10 octobre 2012[397], la Cour constitutionnelle a eu à se prononcer sur l'applicabilité à la profession de détectives privés agréés du devoir d'information prévu à l'article 9 de la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel[398]. Dans ce cadre, la Cour a posé une série de questions préjudicielles à la Cour de justice de l'Union européenne.

392 *Ibid.*, points 52-53.
393 C.J.U.E., 11 juillet 2013, *BEST*, aff. C-657/11. Voy. *supra*, n° 5.
394 Les auteurs remercient la Professeure de Terwangne pour la relecture attentive qu'elle a effectuée.
395 Chercheurs au CRIDS.
396 Chercheuses au CRIDS et avocates.
397 C. const., 10 octobre 2012, n° 116/2012.
398 Loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel, *M.B.*, 18 mars 1993, p. 5801.

Elle souhaitait notamment savoir si les États membres disposaient de la liberté de prévoir une exception à l'obligation d'information immédiate de la personne concernée par le traitement de données. La Cour de justice répondit par l'affirmative à cette question et poursuivit en précisant que l'activité d'un détective privé agissant pour un organisme professionnel de droit public ayant pour mission légale de rechercher des manquements à la déontologie d'une profession règlementée (en l'occurrence celle d'agent immobilier) était susceptible d'être exemptée de certaines obligations prévues dans la directive 95/46/CE[399]. En date du 3 avril 2014, l'affaire est revenue devant la Cour constitutionnelle[400]. Il lui revenait de déterminer si, en ne faisant pas figurer cette exception au devoir d'information pour les détectives privés agréés dans la législation fédérale relative à la protection des données, le législateur belge avait respecté les principes d'égalité et de non-discrimination prévus par la Constitution. Elle aboutit à la conclusion qu'en imposant automatiquement aux détectives privés agréés le devoir d'informer la personne concernée, l'article 9 de loi du 8 décembre 1992 violait les articles 10 et 11 de la Constitution.

97. Vie privée et droit pénal financier. Le 27 mars 2014[401], la Cour constitutionnelle a rendu un arrêt important relatif à l'accès aux données à caractère personnel du contribuable qui sont stockées par l'Administration fiscale.

Le recours en annulation portait sur les articles 8 et 11 de la loi du 3 août 2012 portant dispositions relatives aux traitements de données à caractère personnel réalisés par le Service public fédéral Finances dans le cadre de ses missions.

L'article 8 de la loi créait un service chargé d'assurer l'application de la réglementation relative à la protection de la vie privée par le SPF Finances au sein de celui-ci, ce service étant placé sous l'autorité du plus haut fonctionnaire de ce même SPF. L'article 11 de la loi attaquée prévoyait, pour sa part, une exception au principe d'information garanti par la loi vie privée dans les cas où la personne concernée fait l'objet d'un contrôle ou d'une enquête ou d'actes préparatoires à ceux-ci effectués par le SPF Finances.

La Cour a considéré que l'article 11 devait, d'une part, différencier les données nécessaires aux contrôles et enquêtes de celles étrangères à ces actes et, d'autre part, limiter dans le temps cette exception au droit d'être informé. En conséquence, l'article 11 a été annulé « en ce qu'il permet au responsable du traitement des données de refuser l'exercice des droits garantis par les articles 9, § 2, 10 et 12 de la loi du 8 décembre 1992 "relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel" à l'égard des données personnelles du contribuable qui sont étrangères à l'objet de l'enquête ou du contrôle en cours et en ce qu'il ne prévoit pas de limitation dans le temps de la possibilité de faire exception à l'application de ces droits justifiée par l'accomplissement d'actes préparatoires à un contrôle ou à une enquête »[402]. Par ailleurs, la Cour a précisé qu'il fallait entendre la notion de « préparatifs à une enquête ou contrôle » dans son sens courant qui « implique que des actes indiquant l'intention de l'administration d'ouvrir

399 C.J.U.E., 7 novembre 2013, *Institut professionnel des agents immobiliers (IPI) c. Geoffrey Englebert et autres*, aff. C-473/12.

400 C. const., 3 avril 2014, n° 59/2014.

401 C. const., 27 mars 2014, n° 51/2014. À ce sujet, voy. E. Degrave et A. Lachapelle, « Le droit d'accès du contribuable à ses données à caractère personnel et la lutte contre la fraude fiscale », note sous C. const., 27 mars 2014, *R.G.C.F.*, 2014/5, pp. 322-335.

402 *Ibid.*, p. 15.

une enquête ou de procéder à un contrôle à l'égard d'un contribuable déterminé aient été posés préalablement à la demande de celui-ci d'exercer les droits garantis par la loi du 8 décembre 1992 et qu'une mention de ces actes figure dans le dossier du contribuable »[403]. En d'autres termes, « la demande formulée par le contribuable d'avoir accès aux données personnelles le concernant ne peut pas constituer elle-même l'élément déclencheur d'une enquête ou d'un contrôle à partir duquel l'accès peut lui être refusé »[404].

Pour ce qui concerne l'article 8, la Cour a rejeté le moyen pour des questions de fondement légal du recours dès lors que le recours s'appuyait sur l'article 170 de la Constitution qui ne concernait pas ce moyen et des dispositions de droit international sur lesquelles la Cour ne peut exercer de contrôle. La partie requérante n'avait en effet pas visé l'article 22 de la Constitution dans son recours et ne l'avait invoqué qu'en cours de procédure, ce qui n'est pas admis par la loi.

98. Admissibilité d'une preuve recueillie illégalement au regard de la loi vie privée. L'utilisation par un particulier de caméras dissimulées en vue d'enregistrer les déplacements autour de véhicules et d'identifier les personnes physiques commettant des dégradations à ces derniers constitue une infraction au droit au respect de la vie privée des personnes concernées. À cet égard, la Cour de cassation[405] a eu l'occasion de se prononcer quant à la recevabilité de ces enregistrements vidéo en tant que preuve en appliquant la jurisprudence de l'arrêt *Antigone*[406].

99. Conformément à cette jurisprudence, sauf dans l'hypothèse du non-respect d'une formalité prescrite à peine de nullité, une preuve ne peut être écartée que si son obtention est entachée d'un vice portant atteinte à sa fiabilité ou mettant en péril le droit à un procès équitable. Dans l'arrêt étudié, la Cour a constaté que la loi vie privée ne prescrivait aucune sanction à peine de nullité en cas de preuve recueillie en contravention avec ses dispositions et qu'en l'espèce la fiabilité de la preuve n'a pas été entachée. De même, la Cour a précisé qu'alors que l'atteinte portée au droit au respect de la vie privée de la personne filmée par la caméra était proportionnée au regard des dégâts occasionnés par les infractions, l'atteinte au droit au respect de la vie privée des passants était minime, les caméras étant orientées quasi-exclusivement vers les véhicules. Sur la base de ces éléments, la Cour a conclu que les vidéos enregistrées à l'insu de la personne piégée étaient illégales mais restaient recevables en tant que preuve.

100. Droit à la saine curiosité. Dans le cadre d'une procédure de divorce dont la cour d'appel d'Anvers[407] fut saisie, cette dernière a considéré que la prise de connaissance des e-mails de son conjoint constituait une atteinte au droit au respect de la vie privée au sens de l'article 8 CEDH. Toutefois, ce droit devait être mis en balance avec le droit à la saine curiosité en vertu duquel chaque époux peut s'assurer que les obligations conjugales sont respectées. La cour a, par ailleurs, pris en considération dans son raisonnement le fait que les e-mails en question avaient été échangés entre les conjoints et obtenus de manière régulière.

403 *Ibid.*, 5.3, pp. 10.

404 *Ibid.*, 5.3, pp. 10-11.

405 Cass. (2e ch.), 5 juin 2012, R.G. n° P.11.2100.N, *Pas.*, 2012/6-7-8, pp. 1300-1304.

406 Pour une synthèse récente sur le sujet, voy. N. Colette-Basecqz et I. Bekhouche, « Les dernières évolutions concernant les preuves irrégulières en matière pénale », in *La preuve au carrefour de cinq disciplines juridiques*, Limal, Anthemis, 2013, pp. 9-42.

407 Anvers, 12 mars 2014, *R.A.B.G.*, 2015/4, pp. 267-271.

101. Mariage simulé et droit au respect de la vie privée. Le droit au respect de la vie privée et familiale consacré par l'article 8 CEDH ne protège que le mariage sincère et non simulé. Selon la cour d'appel de Bruxelles, ce droit ne peut être invoqué par un des époux dans une procédure d'annulation de mariage pour absence de consentement dans son chef[408].

102. Relations intimes filmées à l'insu des partenaires. Une personne enregistrant ses relations sexuelles à l'insu de son partenaire est susceptible d'être poursuivie pour attentat à la pudeur[409] mais aussi pour violation de la loi vie privée. À cet égard, la cour d'appel de Mons[410] constate que : « le dossier répressif ne permet pas d'établir que les faits des préventions reprochées au prévenu (…) entrent dans le champ d'application de la loi sur la protection de la vie privée dès lors que l'enquête pénale n'apporte pas la preuve certaine que les objets visés auxdites infractions constituent des "fichiers" au sens de cette législation ». Cette affirmation amène plusieurs commentaires. En premier lieu, se pose la question du sens à donner aux termes « apporter la preuve certaine ». Nul doute qu'il fallait y lire « démontrer » car il ne s'agit pas de prouver la matérialité de faits (les vidéos ayant même été confisquées en première instance) mais de démontrer l'applicabilité de la loi vie privée. En deuxième lieu, il convient de rappeler que la loi vie privée s'applique tant au traitement de données à caractère personnel figurant dans un fichier qu'au traitement automatisé de telles données.

103. Le dossier répressif aurait dû démontrer non seulement que les vidéocassettes pouvaient être considérées comme étant des fichiers (si l'on parle bien de bandes magnétiques classées dans une vidéothèque, *de facto* excluant le traitement automatisé figurant à l'article 1, § 2, de la loi vie privée), mais également que l'enregistrement des données sur les supports informatiques constituait un traitement automatisé de données à caractère personnel. En l'espèce, le prévenu fut acquitté pour les faits portant sur le traitement de données à caractère personnel bien qu'il fût condamné pour avoir porté atteinte à la pudeur de ses partenaires en filmant à leur insu les relations sexuelles « réciproquement » consenties.

104. Droit d'accès aux données d'immatriculation. Dans un arrêt du 11 janvier 2012[411], la Cour constitutionnelle a été amenée à examiner si les concessionnaires chargés de la gestion de parkings publics et les agences communales autonomes étaient habilités à demander l'identité du titulaire d'une plaque d'immatriculation à l'autorité chargée de l'immatriculation des véhicules, et ce, en vue du recouvrement de rétributions ou de taxes de stationnement. En l'espèce, la Cour a considéré que la disposition légale[412] était suffisamment précise, que l'identification du titulaire de la plaque d'immatriculation était, dans ces cas, le seul moyen de déterminer qui était redevable de la taxe ou de la rétribution de stationnement et que l'article en cause prévoyait que cette demande d'identité du titulaire de la plaque devait s'effectuer conformément à la loi vie

408 Bruxelles (3e ch.), 21 mars 2013, *R.T.D.F.*, 2015/2, pp. 246-253.

409 Pour plus de détails sur l'infraction d'attentat à la pudeur, voy. N. Blaise, « L'attentat à la pudeur ou la protection de l'intégrité sexuelle telle qu'elle est communément admise : Commentaire de l'arrêt de la Cour constitutionnelle du 4 juin 2009 », *J.D.J.*, 2009, pp. 19-24.

410 Mons (4e ch.), 14 mars 2013, R.G. n° 148/13, disponible sur http://jure.juridat.just.fgov.be.

411 C. const., 11 janvier 2012, n° 2/2012.

412 Article 10/2 du décret du 16 mai 2008 relatif aux règlements supplémentaires sur la circulation routière et sur la pose et le coût de la signalisation routière, tel que modifié par le décret portant recouvrement de rétributions de stationnement par des sociétés de parking du 9 juillet 2010, *M.B.*, 16 juin 2008, p. 29109.

privée. Elle a dès lors conclu que l'ingérence dans la vie privée répondait à un besoin social impérieux et était proportionnée par rapport à l'objectif poursuivi.

b. Données à caractère personnel relatives à la santé

105. Accès aux données médicales d'une personne décédée[413]**.** La loi du 22 août 2002 relative aux droits du patient[414] prévoit, dans un certain nombre de cas, l'accès par des membres de la famille aux données médicales d'une personne décédée ; disposition qui est intimement liée au respect du droit à la vie privée[415]. La décision rendue par la cour d'appel de Liège[416] illustre l'application correcte de l'article 9, § 4 qui consacre ce droit. En effet, la disposition prévoit quatre conditions cumulatives pour que ce droit puisse être exercé par un proche du défunt : « l'époux, le partenaire cohabitant légal, le partenaire et les parents jusqu'au deuxième degré *inclus ont,* par l'intermédiaire du praticien professionnel *désigné par le demandeur, le droit de consultation* (…) *pour autant que leur* demande soit suffisamment motivée et spécifiée *et que le patient ne s'y soit* pas opposé expressément »[417]. Or, il résulte de l'ensemble des faits rapportés à la cour que le patient s'était manifestement opposé à ce que sa mère accède à ses données médicales, que ce soit de manière générale (volonté de cesser toute relation avec elle en raison de leur relation conflictuelle avérée) ou spécifique (le patient avait confié à son psychologue vouloir qu'aucune donnée ne soit transmise à sa mère). L'article 9, § 4, de la loi susmentionnée n'impose en revanche pas que ce refus soit manifesté sous la forme d'un écrit ; une formulation verbale, tant qu'elle peut être prouvée, suffit. Notons enfin qu'une demande d'accès aux données médicales d'un proche décédé ne peut être refusée par le médecin traitant sous prétexte que le dossier médical est conservé à l'hôpital et que c'est à ce dernier qu'il appartient de communiquer lesdites données. Conformément à l'interprétation faite des travaux préparatoires de la loi, c'est au médecin, et non à l'hôpital, qu'il incombe de veiller à l'équilibre des valeurs en présence et au respect de la volonté de son patient défunt en ce qui concerne la divulgation de son dossier médical à ses proches.

106. Questionnaire médical et proposition d'assurances. Le débat s'inscrit dans le cadre de la souscription, par une personne, d'une assurance « frais médicaux et indemnité journalière d'hospitalisation » auprès d'une compagnie d'assurance et sur les informations qu'elle a dû communiquer dans un questionnaire médical intégré à la proposition d'assurance. La demanderesse avait demandé et obtenu l'écartement du formulaire, la cour ayant estimé qu'en regroupant une proposition d'assurance et un questionnaire médical, la compagnie d'assurance ne garantissait pas le respect de l'article 16, § 4, de la loi vie privée visant à assurer la sécurité des données et de l'article VI.103 du Code de droit économique interdisant les pratiques commerciales déloyales[418].

413 Pour plus de détails sur le sujet, voy. J. Herveg, « La protection des données du patient après son décès : une persistance du droit au respect de la vie privée ? », in *Défis du droit à la protection à la vie privée : Perspective du droit européen et nord-américain*, Bruxelles, Bruylant, 2008, pp. 209-242.

414 Loi du 22 août 2002 relative aux droits du patient, *M.B.*, 26 septembre 2002, p. 43719.

415 À ce propos, il est utile de rappeler que cette loi de 2002 a modifié l'article 10 de la loi vie privée, raison pour laquelle nous reprenons la décision rendue par la cour d'appel de Liège dans la présente chronique.

416 Liège, 4 septembre 2014, R.G. n° 2013/RG/735, disponible sur http://jure.juridat.just.fgov.be.

417 Nous soulignons.

418 Anciennement l'article 94 de la loi relative aux pratiques du marché et à la protection du consommateur.

Par ailleurs, la cour a considéré qu'en autorisant le médecin-conseil de la compagnie d'assurance à consulter son médecin traitant, la demanderesse avait donné son consentement à ce qu'il accède à son dossier médical. Or, les rapports médicaux indiquaient que les informations qu'elle avait fournies à la compagnie dans le formulaire et relatives à son poids et à sa taille étaient fausses. Ces informations constituant des éléments d'appréciation du risque pour l'assureur, il revenait à l'assuré de les fournir spontanément et loyalement. Finalement, dans cet arrêt du 17 septembre 2013, la cour d'appel de Mons a constaté la nullité du contrat d'assurance en application de l'article 7 de la loi du 25 juin 1992[419].

c. Liberté de la presse et vie privée

107. Personnalité publique et droit au respect de la vie privée. Trouver l'équilibre entre la liberté de la presse et la protection de la vie privée est souvent un exercice périlleux auquel doit se livrer le juge, notamment en matière de presse « people ». Tel fut le cas dans le jugement rendu par la juridiction saisie[420] au sujet de photos prises lors des funérailles d'un animateur radio et télévision de la R.T.B.F. sur lesquelles apparaissent sa femme, présentatrice du journal télévisé de la même chaîne, et ses enfants et ce, malgré que la famille ait souhaité que cet événement soit tenu dans la plus stricte intimité.

108. Lesdites photos ont été publiées dans un journal en marge d'un article consacré à la personne décédée. L'article en lui-même n'est pas contesté par les demandeurs, mais bien la juxtaposition de photos prises lors de l'enterrement. Celles-ci contreviendraient au droit au respect à la vie privée et au droit à l'image de la veuve et de ses enfants, ce qui justifie une action à l'encontre du journaliste sur la base des articles 1382 et 1383 du Code civil[421].

109. Les parties défenderesses argumentèrent que l'épouse, en tant que personne de notoriété publique, ne saurait s'opposer à la liberté de la presse pour tout ce qui entre dans le champ de l'intérêt légitime du public en invoquant son droit et celui de ses enfants à la vie privée et à l'image.

110. Le tribunal s'est référé à la jurisprudence de la Cour européenne des droits de l'homme, notamment en utilisant les critères retenus dans les arrêts *Von Hannover*[422]. Dans le contexte de la liberté de la presse, des photos peuvent être publiées sans l'accord de la personne concernée dans l'hypothèse où deux conditions sont cumulativement remplies. D'une part, les photos doivent contribuer, d'une manière ou d'une autre, au débat d'intérêt général. D'autre part, il faut tenir compte de la situation dans laquelle les clichés ont été pris. Si ces derniers ont été obtenus dans des circonstances « douteuses »[423], la vie privée et le droit à l'image de la personne concernée doivent prévaloir.

111. En l'espèce, le tribunal a estimé que les photos et l'article en cause ne nourrissaient nullement une réflexion de fond sur un débat d'intérêt général dans une société démocratique. De plus,

419 Mons (2e ch.), 17 septembre 2013, *J.L.M.B.*, pp. 14-58.

420 Civ. Brabant wallon (1re ch.), 16 octobre 2014, *J.L.M.B.*, 2014, p. 1981.

421 Notons qu'il n'est nullement question d'un délit de presse en espèce mais bien de la responsabilité aquilienne classique compte tenu du fait que la diffusion de photographies prises lors de funérailles ne constitue pas une opinion ou une pensée.

422 Cour eur. D.H., 24 juin 2004 et 7 février 2012, arrêt *Von Hannover c. Allemagne*, req. nos 59320/00, 40660/08 et 60641/08.

423 Civ. Brabant wallon (1re ch.), 16 octobre 2014, *J.L.M.B.*, 2014, p. 1986.

compte tenu du fait que les personnes concernées avaient signifié explicitement leur volonté de se recueillir en toute intimité, notamment en refusant que le décès soit annoncé dans la presse ou par faire-part, le journaliste ne s'est pas comporté comme une personne normalement prudente et diligente. De ce fait, il a commis une faute qui est en lien causal avec le dommage moral subi par les demanderesses.

112. Droit à l'oubli du passé judiciaire. Le droit à l'oubli[424] est une composante intrinsèque du droit au respect de la vie privée (consacré par les articles 8 CEDH et 22 de la Constitution) et peut notamment porter sur le passé judiciaire d'une personne. Il se présente comme « le droit de ne pas voir en permanence rappelé son passé, de ne pas voir son passé encombrer le présent et hypothéquer l'avenir »[425].

113. L'exercice de ce droit doit être encadré par des conditions strictes car il peut s'opposer au droit à la liberté d'expression, autre droit fondamental, consacré par l'article 10 CEDH et par les articles 19 et 25 de la Constitution, tous deux étant d'égale valeur.

114. Ainsi le tribunal de première instance de Bruxelles a considéré que le droit à l'oubli invoqué par la partie demanderesse[426] ne trouvait pas à s'appliquer dans le cas d'un article journalistique décrivant des faits relatifs au mariage d'une personnalité publique dans le milieu social et politique bruxellois. L'article en jeu concernait une question d'intérêt général, à savoir celle des mariages fictifs ou mariages blancs, susceptible de contribuer à un débat public sur des questions de société.

115. Pour traiter cette question d'intérêt général, le journaliste s'appuyait sur un cas particulier et relatait, sans les commenter, des faits privés, dont la divulgation est en principe soumise à autorisation. D'après le tribunal, la mention du nom de la personnalité publique en question et la publication de photographies pour illustrer le propos présentait un intérêt légitime pour le lecteur. Selon ce même tribunal, le droit à l'oubli ne pouvait être reconnu car les trois conditions suivantes n'étaient pas remplies[427] : les faits devaient être de nature judiciaire, ils devaient déjà avoir été divulgués et ils ne pouvaient plus présenter de lien avec l'actualité.

116. Droit à l'oubli numérique[428]. À côté de la divulgation nouvelle et utile de faits judiciaires anciens (droit à l'oubli judiciaire), le droit à l'oubli numérique concerne l'anonymisation, voire la suppression, d'informations maintenues en permanence sur internet.

117. Les faits soumis au tribunal étaient les suivants. Au cours d'un accident de la route causé par un conducteur ivre, deux personnes ont trouvé la mort. Le nom du conducteur a été mentionné dans divers articles de presse de l'époque. Six ans plus tard, le conducteur est réhabilité et deux ans après cette réhabilitation, un article datant de l'époque des faits est mis en ligne

424 Consacré par la Cour de justice de l'Union européenne : C.J.U.E., 13 mai 2014, *Google Spain SL & Google Inc. c. Mario Costeja Gonzáles*, aff. C-131/12.

425 C. de Terwangne, « Droit à l'oubli, droit à l'effacement ? : Quand le législateur et le juge européens dessinent les contours du droit à l'oubli numérique », in *Enjeux européens et mondiaux de la protection des données personnelles*, Bruxelles, Larcier, 2015, p. 273.

426 Civ. Bruxelles (14e ch.), 25 mars 2014, R.G. n° 2013/6156/A.

427 E. Defreyne, « Le droit à l'oubli et les archives journalistiques », *R.D.T.I.*, 2013, n° 51, p. 81.

428 Les auteurs renvoient le lecteur aux parties de la chronique consacrées à la liberté d'expression et aux communications électroniques.

sur le site internet d'un journal national, avec accès gratuit. Le conducteur a sollicité la suppression ou à tout le moins l'anonymisation de l'article publié par le journal en question, sans obtenir satisfaction. Ce faisant, il considère que le journal a violé son droit au respect de la vie privée et lui a causé un dommage moral certain pour lequel il demande et obtient réparation sur la base de l'article 1382 du Code civil[429].

118. Le juge conclut que « la manière la plus efficace de préserver la vie privée du demandeur sans porter atteinte de manière disproportionnée à la liberté d'expression des défenderesses est d'anonymiser l'article litigieux figurant sur le site internet des deux journaux en remplaçant les nom et prénom du demandeur par la lettre X ou les initiales »[430].

119. Le journal – s'estimant censuré par cette décision de justice – a indiqué sous l'article anonymisé en ligne sur son site internet que « toute personne peut néanmoins prendre connaissance de la version intégrale de l'édition originale de l'article d'origine sur simple demande à l'adresse mail droits@rossel.be »[431].

2. Commission de la protection de la vie privée à propos de l'e-gouvernement

Elise Degrave[432]

120. L'e-gouvernement. L'e-gouvernement se caractérise notamment par un nouveau mode de fonctionnement de l'administration fondé sur la collaboration et l'échange maximal des données à caractère personnel des citoyens entre les institutions publiques qui en ont besoin. Il s'agit par-là de simplifier les démarches administratives des citoyens et de renforcer l'efficacité de l'État[433].

121. Dans ce contexte caractérisé notamment par une plus grande opacité de l'administration, la Commission de la protection de la vie privée[434] exerce un rôle primordial pour guider les législateurs et les gouvernements dans la mise en place de l'e-gouvernement. De telles réflexions sont essentielles pour éviter, tant que faire se peut, le développement d'une administration kafkaïenne que le citoyen ne parviendrait ni à comprendre ni à contrôler.

122. Les lignes qui suivent synthétisent les principaux avis que la C.P.V.P. a rendus entre 2012 et 2014 au sujet des outils et des pratiques d'e-gouvernement.

a. Les outils d'e-gouvernement

123. Les intégrateurs de service. Un intégrateur de services est un outil placé au cœur d'un réseau d'administrations, « dans le but de simplifier et d'optimiser les échanges de données entre les différents acteurs publics »[435]. Cet outil est nécessaire pour permettre la concrétisation

429 Liège, 25 septembre 2014, R.G. n° 52013/RG/393, disponible sur http://jure.juridat.just.fgov.be.
430 Civ. Liège (4e ch.), 3 novembre 2014, *J.L.M.B.*, 2014/1, n° 14/964, p. 1969.
431 http://archives.lesoir.be/serie-noire-dans-le-tournaisis-cinq-morts-en-quatre_t-19941110-Z08QYU.html.
432 Assistante à la Faculté de droit de l'Université de Namur et chercheuse au CRIDS (www.crids.eu).
433 À ce sujet, voy. E. Degrave, *L'e-gouvernement et la protection de la vie privée. Légalité, transparence et contrôle*, coll. CRIDS, Bruxelles, Larcier, 2014.
434 Ci-après « C.P.V.P. ».
435 C.P.V.P., avis n° 08/2014 du 5 février 2014 concernant un avant-projet d'ordonnance portant création et organisation d'un intégrateur de services régional, n° 45.

du principe de la collecte unique des données qui consiste « à collecter de manière unique des données auprès de citoyens et d'entreprises pour ensuite stocker ces données dans des sources authentiques, gérées par les autorités publiques, et les rendre accessibles à d'autres instances (publiques) »[436].

124. Ces dernières années ont été créés de nouveaux intégrateurs de services, qualifiés d'intégrateurs de services « horizontaux » ou encore « transversaux ». Ces intégrateurs sont placés au cœur de réseaux d'administrations définis en fonction de l'appartenance desdites administrations à l'entité fédérale ou à une entité fédérée. L'intégrateur de services fédéral, dont la mission est assurée par le SPF Fedict, a été créé par une loi du 15 août 2012[437]. Une loi du 5 mai 2014[438] ajoute, dans la loi du 15 août 2012, l'obligation, pour les administrations du réseau fédéral, de collecter les données disponibles dans ce réseau auprès de Fedict et non plus auprès des personnes concernées. La C.P.V.P. s'est prononcée sur cette modification législative. Après un premier avis défavorable eu égard au fait que, notamment, l'utilisation du numéro d'identification du registre national par l'ensemble des administrations fédérales risquait de ne plus être contrôlé par le comité sectoriel du Registre national[439], la C.P.V.P. s'est prononcée favorablement dans son avis n° 04/2014[440]. Elle y souligne l'importance de maintenir le contrôle *a priori* des échanges de données entre administrations par les comités sectoriels[441]. Elle rappelle que tout citoyen a le droit d'accéder à ses données, non seulement en version électronique mais également en version papier[442]. Et elle insiste sur l'importance de mettre en place un outil de traçage des accès, dit aussi « *audit trail* », permettant d'identifier les personnes ayant eu accès aux données des citoyens[443].

125. Par ailleurs, malgré la multiplication des intégrateurs de services, il faut faire en sorte qu'« un service public ne doive recourir qu'à un seul intégrateur de services » afin de n'être confronté qu'à « un seul système de gestion des utilisateurs et des accès, un seul ensemble de spécifications techniques, etc. »[444]. Des accords doivent donc être conclus entre les intégrateurs de service. La C.P.V.P. propose également des solutions pour respecter la répartition légale des compétences entre services publics, telles que le fait de « reprendre dans l'administration des intégrateurs fédéraux aussi bien des représentants du niveau fédéral que du niveau régional »[445].

436 C.P.V.P., avis n° 03/2014 du 15 janvier 2014 relatif à un avant-projet de loi garantissant le principe de la collecte unique des données dans le fonctionnement des services et instances qui relèvent de ou exécutent certaines missions pour l'autorité fédérale et portant simplification et harmonisation des formulaires électroniques et papier.

437 Loi du 15 août 2012 relative à la création et à l'organisation d'intégrateur de services fédéral, *M.B.*, 29 août 2012.

438 Loi du 5 mai 2014 garantissant le principe de la collecte unique des données dans le fonctionnement des services et instances qui relèvent de ou exécutent certaines missions pour l'autorité et portant simplification et harmonisation des formulaires électroniques et papier, *M.B.*, 4 juin 2014. L'article 13 de cette loi impose la collecte indirecte des données par l'ajout de deux paragraphes à l'article 8 de la loi du 15 août 2012.

439 C.P.V.P., avis n° 03/2014, précité, spéc. concernant les motifs de l'avis défavorable n°s 15 à 17, 22 à 24, 29 à 42, 46, 48 et 49.

440 C.P.V.P., avis n° 04/2014 du 29 janvier 2014 relatif à un avant-projet de loi garantissant le principe de la collecte unique des données dans le fonctionnement des services et instances qui relèvent de ou exécutent certaines missions pour l'autorité fédérale et portant simplification et harmonisation des formulaires électroniques et papier.

441 *Ibid.*, n° 13.

442 *Ibid.*, n° 18.

443 *Ibid.*, n° 21.

444 C.P.V.P., avis n° 08/2014, précité, n° 50.

445 *Ibid.*, n° 52.

126. Autorités de contrôle communautaires et régionales. La C.P.V.P. encourage la création d'autorités qui contrôlent la légalité des échanges de données effectués par l'intermédiaire d'un intégrateur de services communautaire ou régional. Elle rappelle que selon la Cour constitutionnelle et « au regard des compétences implicites visées à l'article 10 de la loi spéciale, les Régions et les Communautés [sont compétentes pour] installer une autorité de contrôle de l'échange des données au sein de leur propre administration »[446]. Ces autorités doivent toutefois respecter la loi du 8 décembre 1992 qui « selon la Cour constitutionnelle, (…) est la réglementation fédérale générale qui a valeur de réglementation minimale pour toute la matière »[447]. La C.P.V.P. est donc favorable à la création de la Commission de contrôle bruxelloise[448] et de la Commission Wallonie-Bruxelles de contrôle des échanges de données[449].

127. L'avis n° 31/2013[450] porte sur l'octroi de nouvelles compétences à la Commission de contrôle flamande pour l'échange électronique de données administratives (ci-après « VTC »[451]), qui souhaite contrôler le respect du décret du 18 juillet 2008[452] et en sanctionner les violations. Dans cet avis, la C.P.V.P. insiste sur l'importance de maintenir un travail préventif de cette autorité pour accompagner les responsables de traitement dans cette matière complexe[453]. Elle reconnaît toutefois le caractère efficacement dissuasif de l'existence de sanctions[454]. Des limites doivent néanmoins encadrer ces sanctions. Celles-ci « ne peuvent constituer que la dernière étape du contrôle administratif »[455]. Avant de se voir imposer une sanction, le responsable du traitement doit pouvoir faire valoir son droit à la défense[456]. La sanction infligée doit être proportionnée à l'illégalité commise. « Il est préférable par exemple d'adapter le flux de données plutôt que de le suspendre, son arrêt étant la dernière solution à envisager (…) à savoir (…) si des intérêts de personnes physiques sont réellement compromis ou si l'on constate un refus manifeste de se conformer aux exigences légales et réglementaires »[457]. Enfin, des recours doivent être organisés contre ces sanctions[458].

128. Sources authentiques de données. Comme le rappelle la C.P.V.P., « les sources authentiques occupent (…) avec les intégrateurs de services (…) une position cruciale dans le contexte

446 *Ibid.*, n° 68.
447 *Ibid.*, n° 21 et les références citées. Cette jurisprudence de la Cour constitutionnelle est discutable. Voy. E. Degrave, « L'article 22 de la Constitution et les traitements de données à caractère personnel », *J.T.*, 2009, pp. 365 à 371.
448 C.P.V.P., avis n° 08/2014, précité.
449 C.P.V.P., avis n° 34/2014 du 30 avril 2014 concernant un projet d'accord de coopération entre la Région wallonne et la Communauté française portant exécution de l'Accord de Coopération du 23 mai 2013 entre la Région wallonne et la Communauté française portant sur le développement d'une initiative commune en matière de partage de données et sur la gestion conjointe de cette initiative.
450 C.P.V.P., avis n° 31/2013 du 17 juillet 2013 relatif à la proposition de décret modifiant le décret du 18 juillet 2008 relatif à l'échange électronique de données administratives, en ce qui concerne la détermination des compétences de surveillance et de contrôle de la Commission de contrôle flamande pour l'échange électronique de données administratives.
451 Vlaamse Toezichtcommissie voor het eletktronische bestuurlijke gegevensverkeer.
452 Décret du 18 juillet 2008 relatif à l'échange électronique de données administratives.
453 C.P.V.P., avis n° 31/2013, précité, n° 17.
454 *Ibid.*, n° 18.
455 *Ibid.*, n° 19.
456 *Ibid.*, n° 20.
457 *Ibid.*, n° 21.
458 *Ibid.*, n° 23.

de l'e-government belge, et cela transparaît aussi de plus en plus dans la réglementation de la matière »[459]. Eu égard au fait que ces bases de données enregistrent certains types de données des citoyens dans le but de les rendre disponibles pour les instances publiques qui en ont besoin[460], elles peuvent avoir un impact négatif important sur la protection de la vie privée des individus si elles ne respectent pas certaines garanties.

129. Dans sa recommandation n° 09/2012 qu'elle a adopté d'initiative, la C.P.V.P. synthétise les exigences qui s'imposent aux sources authentiques de données. La finalité poursuivie par la source authentique doit être déterminée, explicite et légitime, et servir de base à l'examen de compatibilité en cas de réutilisation des données concernées[461]. L'exigence de proportionnalité doit également être respectée, en recueillant autant que possible les données de manière unique[462]. En outre, des moyens doivent être mis en place pour garantir l'exactitude des données au risque de créer un « effet domino » d'une erreur affectant une donnée qui sera réutilisée de multiples fois[463]. Enfin, la transparence des données pour les personnes concernées et la mise en place d'une politique de sécurité des données ne doivent pas être négligées[464].

b. Les pratiques d'e-gouvernement

Nombre de pratiques administratives sont désormais irriguées par l'utilisation des technologies, rendant nécessaire une relecture des principes fondamentaux applicables aux acteurs publics. En particulier, l'usage des technologies dans le secteur public permet à l'État de contrôler plus efficacement les citoyens. Il facilite également nombre de démarches administratives.

§ 1. Le renforcement du contrôle des citoyens

130. La lutte contre la fraude sociale. La C.P.V.P. a dégagé des lignes directrices pour les échanges de données effectués aux fins de lutter contre la fraude sociale[465]. Elle affirme qu'il « faut éviter la concentration d'informations dans une banque de données supplémentaire ». Il est préférable de recourir à la Banque-carrefour de la sécurité sociale « qui évite la concentration des données et qui permet sans doute plus efficacement, si un fichier central était constitué, de connecter entre elles toutes les bases de données existantes dès lors que cette interconnexion poursuit une finalité légitime, ce qu'est la lutte contre la fraude sociale »[466]. La C.P.V.P. rappelle également la nécessité d'obtenir une autorisation de principe, de la part du comité sectoriel de la sécurité sociale, « pour toute communication de données à caractère personnel par la BCSS ou par des institutions de sécurité sociale à d'autres instances situées dans ou à l'extérieur du

459 Recommandation n° 09/2012 du 23 mai 2013 d'initiative relative aux sources authentiques de données dans le secteur public, n° 2.

460 Au sujet de la notion de « donnée authentique », voy. C.P.V.P., avis n° 23/2013 du 26 juin 2013 relatif au projet d'arrêté royal déterminant les critères sur la base desquels des données sont qualifiées d'authentiques en exécution de la loi du 15 août 2012 relative à la création et à l'organisation d'un intégrateur de services fédéral.

461 *Ibid.*, n^os^ 9 à 12.

462 *Ibid.*, n^os^ 13 à 16.

463 *Ibid.*, n^os^ 17 à 22.

464 *Ibid.*, n^os^ 23 à 26.

465 Recommandation n° 01/2012 du 18 janvier 2012 concernant la possibilité d'un inventaire des banques de données pertinentes et d'une amélioration de l'échange d'informations dans le cadre de la lutte contre la fraude sociale.

466 *Ibid.*, n^os^ 26 et 27.

réseau »[467]. Enfin, la C.P.V.P. insiste sur « l'importance qu'une information claire et détaillée soit communiquée aux personnes dont les données seront traitées dans le cadre de la lutte contre la fraude sociale »[468].

131. La lutte contre les immeubles inoccupés. « Les données à caractère personnel relatives aux propriétaires de logements pour lesquels les services de distribution identifient une consommation d'eau inférieure à 5 m^3 par an ou d'électricité de moins de 100 kw par an peuvent [-elles] être communiquées à l'administration bruxelloise compétente » ? Telle était la question à laquelle la C.P.V.P. a répondu dans son avis n° 12/2012[469]. La C.P.V.P. y répond affirmativement. Selon elle, le traitement de données est légal puisqu'il est « nécessaire au respect d'une obligation à laquelle est soumis le responsable du traitement par ou en vertu d'une loi (…) (article 5, c, [de la loi du 8 décembre 1992]) »[470]. La finalité poursuivie respecte également l'article 4, § 1, 2°, de la loi du 8 décembre 1992 puisqu'une ordonnance de la Région bruxelloise du 17 juillet 2003 présume inoccupés, entre autres, « les logements pour lesquels la consommation d'eau ou d'électricité constatée pendant une période d'au-moins douze mois consécutifs est inférieure à la consommation minimale fixée par le Gouvernement »[471]. Seules certaines données à caractère personnel seront transmises par les services de distribution d'eau et l'électricité. La C.P.V.P., moyennant le respect de certaines conditions, estime que l'exigence de proportionnalité est ainsi respectée[472]. S'agissant du devoir d'information des personnes concernées, le service qui réclame les données de consommation en est dispensé, conformément à l'article 9, § 2, de la loi du 8 décembre 1992. Enfin, les données collectées ne pourront être conservées que jusqu'au paiement de l'amende administrative[473].

132. Les sanctions administratives communales. Dans deux avis, la C.P.V.P. s'est prononcée favorablement quant à l'utilisation des données à caractère personnel des citoyens dans le but d'infliger des sanctions administratives communales[474]. Dans son avis n° 04/2013, la C.P.V.P. insiste sur l'importance de désigner le responsable de traitement de la base de données dénommée « registre des sanctions communales administratives », en particulier quand un seul registre est ouvert pour plusieurs communes[475]. Elle attire également l'attention du législateur sur l'importance de déterminer quelle autorité a accès à ces données. « Des données concernant une infraction commise dans une commune A peuvent-elles par exemple être utilisées dans une commune B afin de pouvoir prouver une "récidive" et ainsi infliger une amende plus élevée ? »[476].

467 *Ibid.*, n° 36.

468 *Ibid.*, n° 32.

469 Avis n° 12/2012 du 11 avril 2012 relative à la communication de données de consommation d'eau et d'électricité par les services de distribution à la Cellule administrative régionale *ad hoc* de la Région de Bruxelles-Capitale dans le cadre de la lutte contre les immeubles inoccupés.

470 *Ibid.*, n° 8.

471 *Ibid.*, n° 15.

472 *Ibid.*, n^{os} 17 à 29.

473 *Ibid.*, n° 36.

474 C.P.V.P., avis n° 04/2013 du 30 janvier 2013 relatif à un avant-projet de loi relatif aux sanctions administratives communales et visant à lutter contre les incivilités ; avis n° 56/2013 du 6 novembre 2013 concernant le projet d'arrêté royal fixant les conditions particulières relatives au registre des sanctions administratives communales institué par l'article 44 de la loi du 24 juin 2013 relative aux sanctions administratives communales.

475 C.P.V.P., avis n° 04/2013, n^{os} 10 et 11.

476 *Ibid.*, n° 12.

D'amples considérations sont également consacrées à l'information des personnes concernées. En particulier, une commune, en tant que responsable de traitement dans le cadre de la législation sur les sanctions administratives, ne peut invoquer la dispense au devoir d'information telle qu'elle figure à l'article 3, § 5, de la loi du 8 décembre 1992[477]. Par ailleurs, la C.P.V.P. rappelle que chaque citoyen a le droit de consulter son dossier et de faire rectifier les données erronées[478].

§ 2. La simplification des démarches administratives

133. Application numérique et démarche administrative. L'administration souhaite disposer d'applications numériques pour effectuer des démarches administratives en ligne. Dans son avis n° 20/2014, la C.P.V.P. constate que « l'utilisation croissante des tablettes et des smartphones confronte l'administration au défi d'également pouvoir offrir sur ces nouveaux appareils l'accès aux applications publiques numériques, toujours plus nombreuses »[479]. À cette fin, il y a lieu de trouver des solutions pour permettre une identification plus aisée du citoyen à partir de sa carte d'identité électronique. On pourrait, pour ce faire, s'inspirer des moyens d'identification sans fil des systèmes de banque à domicile[480]. Cet avis se concentre sur les mesures techniques et organisationnelles qui doivent être mises en place pour assurer un niveau de protection adéquat lors de l'identification des citoyens. Elle recommande notamment que le projet d'arrêté royal « entre moins dans les détails et notamment qu'il prévoie simplement les fonctionnalités auxquelles le système visé devra satisfaire »[481].

3. *Cour de justice de l'Union européenne (Cour de justice, Tribunal et Tribunal de la fonction publique)*

Claire Gayrel[482]

134. Introduction. La période couverte par cette chronique de jurisprudence pour ce qui concerne les juridictions de l'Union européenne est marquée par deux arrêts fondamentaux, et très remarqués, rendus par la Cour de justice. Outre leur intérêt dans le domaine de la protection des données, ces arrêts marquent l'évolution de la Cour de Luxembourg dans sa fonction de juge des droits fondamentaux. Il s'agit de la décision *Digital Rights Ireland*[483] portant annulation de la directive 2006/24 relative à la conservation des données de trafic et de la décision *Google Spain*[484] consacrant, dans certaines limites, un droit à l'oubli numérique[485]. Nous commencerons

477 *Ibid.*, n° 17.

478 *Ibid.*, n° 24.

479 C.P.V.P., avis n° 20/2014 du 19 mars 2014 concernant le projet d'arrêté royal fixant les conditions, la procédure et les conséquences de l'agrément de services d'identification pour applications publiques numériques qui utilisent des moyens d'identification sans fil, n° 5.

480 *Ibid.*, n° 6.

481 *Ibid.*, n° 9.

482 Chercheur au CRIDS.

483 C.J.U.E. (gr. ch.), 8 avril 2014, *Digital Rights Ireland*, aff. C-293/12. Pour plus d'informations, voy. E. Guild et S. Carrera, « The Political and Judicial Life of Metadata : Digital Rights Ireland and the Trail of the Data Retention Directive », *CEPS Paper for Liberty and Security*, n° 65, mai 2014 ; I. Chatelier et M.-V. Perez Asinari, « Arrêt "Digital Rights Ireland" : invalidité de la directive sur la conservation des données de trafic », *J.D.E.*, 2014, pp. 250-252.

484 C.J.U.E., 13 mai 2014, *Google Spain SL & Google Inc. c. Mario Costeja Gonzáles*, aff. C-131/12.

485 Voy. notamment les commentaires de E. Defreyne et R. Robert, « C.J.U.E., *Google Spain SL, Google Inc. v Agencia Española de Protección de Datos*, 13 mai 2014, aff. C-131/12 », *R.D.T.I.*, 2014, n° 56, pp. 53-114 et de C. de Terwangne, « Droit à l'oubli,

cette chronique par les décisions faisant application des droits fondamentaux relatifs à la protection de la vie privée et des données à caractère personnel reconnus respectivement aux articles 7 et 8 de la Charte des droits fondamentaux (a). Après avoir présenté les positions des juridictions quant aux notions de traitement et de données à caractère personnel (b), nous présenterons les décisions portant sur l'interprétation de dispositions de la directive 95/46[486], notamment en ce qui concerne son champ d'application (c), les principes et droits applicables (d) et l'indépendance des autorités de contrôle (e). Enfin, nous examinerons la jurisprudence relative à la directive 2002/58[487] (f) et à la protection des données traitées par les institutions de l'Union en application du règlement n° 45/2001[488] (g) pertinents pour notre chronique.

a. L'application du droit fondamental à la vie privée et à la protection des données

135. L'invalidité de la directive relative à la conservation des données de trafic. Saisie de demandes préjudicielles introduites par la High Court (Irlande) et le Verfassungsgerichtshof (Autriche), la Cour a annulé la directive 2006/24 relative à la conservation des données de trafic[489], au regard de leur invalidité avec les droits reconnus aux articles 7 et 8 de la Charte. Pour rappel, la directive 2006/24 avait pour objectif d'harmoniser les dispositions nationales relatives à la conservation, pour une durée de six mois à deux ans, par les fournisseurs de services de communications accessibles au public ou de réseaux publics de communications, de l'ensemble des données de trafic (mobile, fixe, téléphonie par internet et internet), en vue de garantir leur disponibilité à des fins de prévention, recherche, détection et poursuite d'infractions graves. Cette annulation intervient huit ans après l'adoption de la directive, alors que les lois nationales de transposition avaient déjà suscité un contentieux national important. Il est notable que l'effet de cette annulation vaut *ab initio*, entraînant aussi le remboursement de l'amende payée par la Suède suite à sa condamnation pour transposition tardive de la directive[490]. Toutefois, l'arrêt de la Cour ne vaut que pour le droit de l'Union et laisse intactes les mesures de droit national existantes[491].

droit à l'effacement ? : Quand le législateur et le juge européens dessinent les contours du droit à l'oubli numérique », in *Enjeux européens et mondiaux de la protection des données personnelles*, Bruxelles, Larcier, 2015, pp. 245-275. Sur le droit à l'oubli, voy. égal. *infra*, n^os^ 304 et s.

486 Directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 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, *J.O.C.E.* L 281 du 23 novembre 1995.

487 Directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive « vie privée et communications électroniques », *J.O.C.E.* L 201 du 31 juillet 2002.

488 Règlement (CE) n° 45/2001 du Parlement européen et du Conseil du 18 décembre 2000 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions et organes communautaires et à la libre circulation de ces données, *J.O.C.E.* L 8 du 12 janvier 2001.

489 Directive 2006/24/CE du Parlement européen et du Conseil du 15 mars 2006 sur la conservation de données générées ou traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public ou de réseaux publics de communications, et modifiant la directive 2002/58/CE, *J.O.U.E.* L 105 du 13 avril 2006.

490 C.J.U.E., 30 mai 2013, *Commission c. Suède*, aff. C-270/11.

491 Pour plus d'informations sur les conséquences de l'arrêt *Digital Rights Ireland* sur les mesures nationales de transposition, voy. notamment A. Wiedman, « Le dialogue sur les droits fondamentaux entre la Cour de justice et les juridictions nationales après l'arrêt *Digital Rights Ireland et Seitlinger e.a.* », *R.A.E.-L.E.A.*, 2014/2, pp. 423-432 et F. Boehm et M. D. Cole, « Data Retention After the Judgement of the Court of Justice of the European Union », 30 juin 2014, Rapport commandé par le député européen J.-P. Albreicht, disponible sur www.janalbrecht.eu/fileadmin/material/Dokumente/Boehm_Cole_-_Data_Retention_Study_-_June_2014.pdf.

La pertinence des articles 7 et 8 de la Charte est établie par la Cour en raison du fait que les données de trafic « prises dans leur ensemble, sont susceptibles de permettre de tirer des conclusions très précises concernant la vie privée des personnes dont les données ont été conservées… »[492]. La Cour distingue ensuite l'ingérence occasionnée par la conservation des données, de l'ingérence occasionnée par l'accès auxdites données de trafic[493]. S'il n'est pas porté atteinte au contenu essentiel des droits fondamentaux protégés aux articles 7 et 8 de la Charte[494], elle considère qu'eu égard à l'ampleur et à la gravité de l'ingérence, la Cour est appelée à exercer un contrôle de légalité strict[495]. Dans son analyse de proportionnalité, la Cour va d'abord considérer, sans surprise, que la mesure remplit la condition d'appropriation, en ce sens que la conservation des données de trafic peut être considérée comme apte à contribuer à l'élucidation d'infractions graves[496]. En revanche, la Cour va juger que la mesure ne saurait être considérée comme limitée au strict nécessaire. Trois arguments principaux sont développés. En premier lieu, la Cour soulève le problème de la rétention globale, sans distinction, différentiation, ni exception, des données de trafic[497]. En particulier, est visée ici la conservation de données relatives à des personnes pour lesquelles « il n'existe aucun indice de nature à laisser croire que leur comportement puisse avoir un lien, même indirect ou lointain, avec des infractions graves ». Par ailleurs, la Cour relève l'absence d'exceptions pour les personnes soumises au secret professionnel, ainsi que l'absence de limites temporelles, géographiques ou personnelles à cette conservation, et l'absence d'exigence d'une relation entre les données à conserver et une menace spécifique à la sécurité publique. En deuxième lieu, la Cour souligne que la directive ne prévoit aucun critère objectif délimitant le pouvoir d'accès des autorités nationales compétentes[498]. Ici, la Cour juge insatisfaisant le renvoi au droit national, considérant que c'était au législateur européen lui même de prévoir les garanties, et notamment procédurales, organisant l'accès et l'utilisation des données. Enfin, la Cour critique la durée de conservation, dont la nécessité n'est pas suffisamment établie[499].

136. La validité du passeport biométrique européen. La Cour a eu à examiner la validité du passeport biométrique européen, contenant une photo faciale et deux empreintes digitales[500]. Reconnaissant que le prélèvement et la conservation d'empreintes digitales par les autorités nationales constituent une atteinte aux droits au respect de la vie privée et à la protection des données à caractère personnel, la Cour a ensuite considéré que cette mesure était proportionnée aux buts poursuivis, à savoir prévenir la falsification des passeports et empêcher leur utilisation frauduleuse[501]. Après avoir discuté les alternatives disponibles telle que la reconnaissance de l'iris, la Cour a finalement admis qu'il n'avait pas été porté à sa connaissance l'existence de mesures

492 C.J.U.E. (gr. ch.), 8 avril 2014, *Digital Rights Ireland*, précité, point 27.
493 *Ibid.*, points 34 et 35.
494 *Ibid.*, points 39 et 40.
495 *Ibid.*, point 48.
496 *Ibid.*, points 49 et 50.
497 *Ibid.*, points 57 à 59.
498 *Ibid.*, points 60 à 62.
499 *Ibid.*, points 63 et 64.
500 En particulier l'article 1, paragraphe 2, du règlement n° 2252/2004 du Conseil du 13 décembre 2004 établissant des normes pour les éléments de sécurité et les éléments biométriques intégrés dans les passeports et les documents de voyage délivrés par les États membres, *J.O.C.E.* L 385 du 29 décembre 2004.
501 C.J.U.E., 17 octobre 2013, *Michael Schwarz c. Stadt Bochum*, aff. C-291/12.

alternatives susceptibles de contribuer, de manière suffisamment efficace, au but poursuivi[502]. Dans ce cadre, le prélèvement d'empreintes digitales doit être considéré comme valide. Enfin, concernant l'argument soulevé tenant au risque d'utilisation ultérieure des empreintes digitales qui seraient conservées de manière centralisée par les États membres à d'autres fins, la Cour affirme que la validité de telles mesures devrait être examinée par les juridictions nationales, puisque le règlement ne prévoit pas de conservation centralisée des empreintes[503].

b. Notions de données à caractère personnel, de traitement et de responsable de traitement

137. Traitement de données à caractère personnel soumis auxdites réglementations. Conduites à interpréter des dispositions de la directive 95/46 ou du règlement n° 45/2001, les juridictions de l'Union ont eu à vérifier au préalable, de manière plus ou moins évidente, si elles se trouvaient effectivement en présence d'un traitement de données à caractère personnel soumis auxdites réglementations. L'examen fait par les juridictions de ces notions est en effet essentiel pour déterminer le champ d'application matériel des textes et donc, de l'étendue de la protection qu'ils confèrent.

La Cour de justice a constaté que les données figurant dans un registre du temps de travail concernant, pour chaque travailleur, les périodes de travail et de repos constituaient des données à caractère personnel et que leur collecte, enregistrement, organisation, consultation, utilisation et transmission étaient un traitement de données[504]. Dans une autre affaire, la Cour a évidemment reconnu que les collecte, conservation et transmission de données portant sur des personnes physiques par des détectives privés équivalaient bien à un traitement[505], ainsi que les activités de vidéosurveillance, en particulier l'enregistrement d'images captées par caméra sur un disque dur[506]. Le Tribunal a quant à lui précisé que l'information permettant d'identifier personnellement les auteurs de certaines observations, en l'espèce l'information reliant chaque observation à l'expert qui l'a émise, constituait une données à caractère personnel[507].

Dans le cas des activités des moteurs de recherche[508], la Cour a observé que « les données trouvées, indexées, stockées par les moteurs de recherche et mises à la disposition de leurs utilisateurs » concernent pour partie des données à caractère personnel et que les activités d'exploration d'internet automatisée, constante et systématique à la recherche des informations qui y sont publiées par l'exploitant d'un moteur de recherche en vue de leur collecte, de leur enregistrement sur ses serveurs, de leur organisation au moyen d'un programme d'indexation et enfin de leur communication aux utilisateurs constituent indubitablement des traitements de données visés à l'article 2, b), de la directive 95/46. Plus discutée était la question de savoir si Google était « responsable de traitement », alors que ce dernier n'a pas de contrôle sur les données publiées

502 *Ibid.*, point 53.
503 *Ibid.*, point 62.
504 C.J.U.E., 30 mai 2013, *Worten*, aff. C-342/12, points 19 et 20 ; C.J.U.E., 19 juin 2014, *Pharmacontinente – Saude e Higiene SA*, aff. C-683/13, point 12.
505 C.J.U.E., 7 novembre 2013, *Institut Professionnel des agents immobiliers (IPI)*, aff. C-473/12, point 26.
506 C.J.U.E., 11 décembre 2014, *František Ryneš c. Úřad pro ochranu osobních údajů*, aff. C-212/13, point 25.
507 T.U.E., 13 septembre 2013, *ClientEarth & Pesticide Action Network Europe (PAN Europe) c. Autorité européenne de sécurité alimentaire (EFSA)*, aff. T-214/11, point 46.
508 C.J.U.E. (gr. ch.), 13 mai 2014, *Google Spain SL c. Mario Costeja Gonzàles*, aff. C-131/12.

sur les pages web de tiers. Pour la Cour, « le traitement de données à caractère personnel effectué dans le cadre de l'activité d'un moteur de recherche se distingue de et s'ajoute à celui effectué par les éditeurs de sites web, consistant à faire figurer ces données sur une page internet »[509]. Dans ce cadre, les moteurs de recherche jouent un rôle décisif dans la diffusion globale desdites données[510] et leurs activités sont donc susceptibles « d'affecter significativement et de manière inconditionnelle par rapport à celle des éditeurs de sites web les droits fondamentaux de la vie privée et de la protection des données à caractère personnel »[511]. Dès lors, pour que les garanties apportées par la directive 95/46 puissent développer leur plein effet, il revient à l'exploitant d'un moteur de recherche en tant que personne déterminant les finalités et les moyens de cette activité et « dans le cadre de ses responsabilités, de ses compétences et ses possibilités » d'assurer le respect de la directive 95/46[512].

Enfin, le T.F.P. et la Cour ont adopté une approche restrictive de la notion de « données à caractère personnel » suivant un raisonnement assez proche consistant à lier la qualification de donnée à caractère personnel aux droits des personnes concernées. Le T.F.P. était saisi d'un recours, visant à annuler la décision du jury de l'EPSO[513] de ne pas inscrire le demandeur sur la liste des lauréats à un concours[514]. Le Tribunal a considéré que de tels documents étaient couverts par le secret du jury, rejetant les arguments tirés d'une violation de l'article 8 de la Charte et du règlement n° 45/2001. En effet, pour ce dernier « par données personnelles sont uniquement visées les informations susceptibles de permettre l'identification d'une personne. Il s'ensuit qu'en vertu des dispositions précitées, le requérant est en droit d'obtenir un accès aux données détenues par l'EPSO permettant de l'identifier et non un accès à sa copie corrigée, aux questions sur lesquelles il a échoué, aux raisons pour lesquelles ses réponses étaient erronées ou à la grille d'évaluation utilisée. Il en est d'autant plus ainsi que, s'il devait être considéré que la copie corrigée d'un candidat constitue une donnée personnelle, ce dernier pourrait, conformément à l'article 14 du règlement n° 45/2001, demander à ce que celle-ci soit rectifiée, ce qui serait absurde »[515].

La Cour a de son côté jugé que si les données collectées et reproduites dans un document préparatoire à l'adoption d'une décision administrative relative à une demande de titre de séjour sont bien des données à caractère personnel, l'analyse juridique qui est établie au moyen de ces données par le fonctionnaire préparant la décision n'est pas une donnée à caractère personnel[516]. Pour la Cour, « une telle analyse juridique constitue non pas une information concernant le demandeur du titre de séjour, mais tout au plus, pour autant qu'elle ne se limite pas à une interprétation purement abstraire du droit, une information portant sur l'appréciation et l'application, par l'autorité compétente, de ce droit à la situation de ce demandeur, cette situation étant notamment établie au moyen des données à caractère personnel relatives à sa personne »[517]. Selon la Cour, les droits de la personne concernée, visés par la directive 95/46 impliquent, notamment, que cette personne

509 *Ibid.*, point 35.
510 *Ibid.*, point 36.
511 *Ibid.*, point 38.
512 *Ibid.*
513 European Personnel Selection Office.
514 T.F.P., 12 février 2014, *Gonzalo de Mendoza Asensi c. Commission européenne*, F-127/11.
515 *Ibid.*, point 101.
516 C.J.U.E., 17 juillet 2014, *Y.S., M. & S. c. Minister voor Immigratie, Integratie en Asiel*, aff. jointes C-141/12 et C-372/12.
517 *Ibid.*, point 40.

puisse s'assurer que les données à caractère personnel la concernant sont exactes et qu'elles sont traitées de manière licite. Le droit d'accès vise donc à permettre à la personne concernée d'effectuer les vérifications nécessaires, et le cas échéant d'obtenir la rectification, l'effacement ou le verrouillage des données[518]. « Or contrairement aux données relatives au demandeur du titre de séjour (…) l'analyse juridique n'est pas en elle-même susceptible de faire l'objet d'une vérification de son exactitude par ce demandeur et d'une rectification au titre de l'article 12, sous b), de la directive 95/56 »[519]. La Cour abonde donc dans le sens du T.F.P. en liant étroitement la qualification de donnée à caractère personnel aux droits de la personne concernée, notamment en matière de rectification. Cette approche constitue selon nous une interprétation trop étroite de la notion de données à caractère personnel puisque l'octroi de l'accès à la personne concernée n'est pas nécessairement associé au droit de rectification, qui n'est octroyé que pour des « données incomplètes ou inexactes »[520].

c. Champ d'application

138. Champ d'application territorial. Dans l'affaire *Google Spain*, il s'agissait de déterminer si l'activité d'indexation, bien que réalisé par Google Search, dont le siège se situe en dehors du territoire de l'Union, tombait ou non dans le champ d'application territorial de la directive 95/46. En effet, c'est la filiale Google Spain dont les activités se limitent à la promotion et la vente de produits et services de publicité en ligne en Espagne qui se trouvait en cause, alors même que l'activité d'indexation, et donc le traitement de données à caractère personnel caractérisé plus tôt par la Cour (voy. *supra*), n'était pas réalisé par Google Spain. La Cour a rappelé que la directive 95/46 vise à s'appliquer aux traitements de données à caractère personnel effectués « dans le cadre » des activités d'un établissement du responsable de traitement sur le territoire d'un État membre, et pas seulement aux traitements effectués « par » cet établissement[521]. En l'espèce, la Cour considère que « les activités de l'exploitant du moteur de recherche et celles de son établissement situé dans l'État membre concerné sont indissociablement liées dès lors que les activités relatives aux espaces publicitaires constituent le moyen pour rendre le moteur de recherche en cause économiquement rentable et que ce moteur est, en même temps, le moyen permettant l'accomplissement de ces activités »[522]. Dès lors, la Cour a jugé que « l'article 4, paragraphe 1, sous a), de la directive 95/46 doit être interprété en ce sens qu'un traitement de données à caractère personnel est effectué dans le cadre des activités d'un établissement du responsable de ce traitement sur le territoire d'un État membre, au sens de cette disposition, lorsque l'exploitant d'un moteur de recherche crée dans un État membre une succursale ou une filiale destinée à assurer la promotion et la vente des espaces publicitaires par ce moteur et dont l'activité vise les habitants de cet État membre »[523].

139. Portée de l'exception des traitements à finalité personnelle et domestique. La Cour a eu l'occasion de rappeler que la protection du droit fondamental à la vie privée tel que garanti à

518 *Ibid.*, point 44.
519 *Ibid.*, point 45.
520 Article 14 du règlement n° 45/2001 ; article 12, sous b), de la directive 95/46.
521 C.J.U.E. (gr. ch.), 13 mai 2014, *Google Spain*, précité, point 52.
522 *Ibid.*, point 56.
523 *Ibid.*, point 60.

l'article 7 de la Charte exige que les dérogations à la protection des données à caractère personnel et les limitations de celle-ci doivent s'opérer dans les limites du strict nécessaire et que l'article 3, § 2, second tiret, de la directive 95/46 doit recevoir une interprétation stricte. Dans ce cadre, elle a jugé que l'exploitation d'un système de caméra installé sur une maison familiale afin de protéger les biens, la santé et la vie des propriétaires de la maison, et dont la surveillance s'étend, même partiellement, à l'espace public, ne peut être considéré comme relevant d'activités exclusivement personnelles et domestiques[524].

d. Principes et droits de la protection des données

140. Légitimité. Dans les affaires *Worten*[525] et *Pharmacontinente*[526], la Cour a jugé qu'une réglementation nationale qui impose à l'employeur l'obligation de mettre à la disposition de l'autorité nationale compétente le registre du temps de travail afin d'en permettre la consultation immédiate, pour autant que cette mesure soit jugée nécessaire pour une application plus efficace de la réglementation, est compatible avec la directive 95/46 et notamment son article 7, sous c) et e), autorisant les traitements de données « nécessaire[s] au respect d'une obligation légale à laquelle le responsable du traitement est soumis » ou « à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique ».

141. Principe de sécurité. Dans l'affaire *Worten* relative à l'accès aux registres du temps de travail par l'autorité nationale du contrôle des conditions de travail, la Cour a jugé qu'il incombe à tout responsable de traitement, conformément à l'article 17, § 1er, de la directive, « d'adopter les mesures techniques et d'organisation nécessaires pour s'assurer que seules des personnes dûment autorisées à accéder aux données à caractère personnel concernées soient en droit de répondre à une demande d'accès émanant d'un tiers »[527].

142. Droit d'accès. La Cour a jugé que l'article 12, sous a), relatif au droit d'accès des individus aux données à caractère personnel les concernant, ne s'opposait pas à la perception de frais, tel qu'un droit de timbre, pour la communication par une autorité publique de données à caractère personnel[528]. Il appartient aux États membres de fixer le montant desdits frais « à un niveau qui constitue un juste équilibre entre d'une part, l'intérêt de la personne concernée à protéger sa vie privée, et (…), d'autre part, la charge que l'obligation de communiquer ces informations représente pour le responsable de traitement »[529]. Toutefois, pour que de tels frais ne soient pas susceptibles de constituer un obstacle à l'exercice du droit d'accès, la Cour indique que « leur montant ne doit pas excéder le coût de la communication de ces données »[530].

143. Quant à la forme que doivent prendre les données communiquées au titre du droit d'accès, la Cour a considéré que « pour qu'il soit satisfait à ce droit, il suffit que le demandeur soit mis en possession d'un aperçu complet de ces données sous une forme intelligible, c'est-à-dire une forme

524 C.J.U.E., 11 décembre 2014, *František Ryneš*, précité, point 35.
525 C.J.U.E., 30 mai 2013, *Worten*, précité, point 45.
526 C.J.U.E., 19 juin 2014, *Pharmacontinente*, précité, point 12.
527 C.J.U.E., 30 mai 2013, *Worten*, précité, point 28.
528 C.J.U.E., 12 décembre 2013, *X*, aff. C-486/12.
529 *Ibid.*, point 28.
530 *Ibid.*, point 31.

permettant à ce demandeur de prendre connaissance desdites données et de vérifier que ces dernières sont exactes et traitées de manière conforme à cette directive, afin qu'il puisse, le cas échéant, exercer les droits qui lui sont conférés par ladite directive »[531]. En l'espèce, le droit d'accès ne confère pas au demandeur d'un titre de séjour le droit d'obtenir une copie du document original ou du fichier original complet dans lequel des données à caractère personnel le concernant figurent, mais porte seulement sur les données relatives au demandeur du titre de séjour[532].

144. Droit d'effacement, d'opposition et droit à l'« oubli ». Après avoir considéré que Google était bien responsable d'un traitement de données à caractère personnel entrant dans le champ d'application de la directive, la Cour devait déterminer si le requérant pouvait solliciter la suppression, par Google, d'un lien de la liste de résultats affichée à partir d'une recherche effectuée sur la base de son nom. Tandis que l'avocat général avait considéré que cette obligation de suppression ne valait qu'à titre subsidiaire, c'est-à-dire après que la personne concernée eut d'abord exercé son droit à l'effacement auprès de l'éditeur de la page web sur laquelle figurerait les informations à supprimer, la Cour à quant elle rejeté une telle approche. Selon la Cour, « compte tenu de la facilité avec laquelle des informations publiées sur un site web peuvent être répliquées (…), une protection efficace et complète des personnes concernées ne pourrait être réalisée si celles-ci devaient d'abord ou en parallèle obtenir l'effacement des informations les concernant auprès des éditeurs de site web »[533].

145. Quant à la portée des droits protégés par l'article 12, sous b) (droit d'effacement « en raison du caractère incomplet ou inexact des données »), ou à l'article 14, alinéa 1, sous a) (droit d'opposition), la Cour ira même plus loin, en considérant que « même un traitement initialement licite de données exactes, peut devenir, avec le temps, incompatible avec cette directive, (…) Tel est notamment le cas lorsque [les données] apparaissent inadéquates, qu'elles ne sont pas ou plus pertinentes ou sont excessives au regard [des finalités initiales du traitement] et du temps qui s'est écoulé ». Dès lors, une information exacte et publiée de manière licite peut perdre sa « pertinence » avec le temps et donc faire l'objet d'une demande d'effacement. Pour la Cour, il n'est pas nécessaire que l'information en question apparaissant dans la liste de résultats cause un préjudice à la personne concernée, cette dernière « pouvant, eu égard à ses droits fondamentaux au titre des articles 7 et 8 de la Charte, demander que l'information en question ne soit plus mise à la disposition du grand public du fait de son inclusion dans une telle liste de résultats ». Si de tels droits « prévalent, en principe, non seulement sur l'intérêt économique de l'exploitant du moteur de recherche, mais également sur l'intérêt de ce public à accéder à ladite information lors d'une recherche portant sur le nom de cette personne », l'équilibre entre vie privée et droit d'accès à l'information devra être recherché en fonction de « la nature de l'information en question, de sa sensibilité pour la vie privée de la personne concernée ainsi que de l'intérêt du public à disposer de cette information, lequel peut varier, notamment, en fonction du rôle joué par cette personne dans la vie publique »[534].

531 C.J.U.E., 17 juillet 2014, *Y.S., M. & S. c. Minister voor Immigratie, Integratie en Asiel*, précité, point 60.

532 *Ibid.*, point 59.

533 C.J.U.E. (gr. ch.), 13 mai 2014, *Google Spain*, précité, point 84.

534 *Ibid.*, point 81. Pour une critique de la décision de la Cour au regard du droit d'accès à l'information, voy. Q. Van Enis, « Le droit de recevoir des informations ou des idées par le biais d'Internet, parent pauvre de la liberté d'expression dans l'ordre juridique européen ? », *J.E.D.H.*, 2015/2, pp. 173-201.

146. Portée des exceptions prévues à l'article 13. Dans le cadre d'un renvoi préjudiciel portant sur l'étendue des exceptions prévues à l'article 13 de la directive, la Cour a rappelé que les États membres disposaient d'une faculté et non d'une obligation de prévoir des exceptions pour les cas visés à l'article 13. Dans le cas qui lui était soumis, la Cour a jugé que « l'activité de détective privé agissant pour un organisme professionnel afin de rechercher des manquements à la déontologie d'une profession règlementée, en l'occurrence celle d'agent immobilier » relevait bien de l'exception prévue à l'article 13, paragraphe 1, sous d)[535].

e. Indépendance des autorités de contrôle

147. Indépendance des autorités de contrôle. Réunie en Grande Chambre, la Cour était saisie de deux requêtes de la Commission européenne contre l'Autriche et la Hongrie visant à établir le manquement de ces deux États à leurs obligations au titre de l'article 28 de la directive 95/46 relatif à l'indépendance des autorités de contrôle[536]. Ce n'est pas la première fois que la Cour de justice est amenée à préciser les garanties d'indépendance attendues pour une autorité nationale de protection des données. Pour rappel, la Cour a déjà jugé que l'Allemagne avait manqué à son obligation en soumettant les autorités de contrôle du secteur non public à la tutelle de l'État[537].

148. Dans le cas de l'Autriche, trois questions principales ont été soulevées. En premier lieu, il s'agissait de déterminer si une tutelle de service restreinte, telle que prévue par la loi de 1979 relative au statut des fonctionnaires et à laquelle le membre administrateur de la Datenschutzkommission (ci-après « DSK », autorité autrichienne de protection des données) est soumis, pouvait être constitutive d'une influence extérieure indirecte, et donc incompatible avec l'objectif d'exercer ses missions « en toute indépendance ». Contre les arguments de l'Autriche et de l'Allemagne pour lesquels une tutelle de service restreinte est conforme à l'article 28, § 1er, de la directive 95/46, mais aussi à la condition d'indépendance inhérente à l'article 267 TFUE, la Cour a considéré que l'indépendance fonctionnelle, entendu en ce sens que les membres ne sont liés par aucune instruction dans l'exercice de leur fonction ne constitue pas une condition à elle seule suffisante pour préserver ladite autorité de toute influence extérieure[538]. En l'espèce, dans la mesure où le membre administrateur de la DSK est un fonctionnaire fédéral issu de la Chancellerie, ses liens de service avec cet organe politique ne permettent pas d'affirmer que la DSK soit au-dessus de tout soupçon de partialité[539]. En deuxième lieu, la Cour a considéré que l'intégration du bureau de la DSK aux services de la Chancellerie fédérale, et notamment le fait que le personnel du bureau de la DSK soit composé de fonctionnaires de la Chancellerie fédérale n'était pas compatible avec l'exigence d'indépendance prévue à l'article 28[540]. Enfin, la Cour a jugé que le droit à l'information très vaste et inconditionnel dont bénéficie le chancelier fédéral auprès du président et du membre administrateur de la DSK prévu par la loi nationale de protection des données ne saurait garantir que la DSK exerce « en toute indépendance » les missions dont elle est investie[541].

535 C.J.U.E., 7 novembre 2013, *Institut Professionnel des agents immobiliers (IPI)*, précité, points 51-53.
536 C.J.U.E. (gr. ch.), 16 octobre 2012, *Commission c. Autriche*, aff. C-614/10.
537 C.J.U.E. (gr. ch.), 9 mars 2010, *Commission c. Allemagne*, aff. C-518/07.
538 C.J.U.E. (gr. ch.), 16 octobre 2012, *Commission c. Autriche*, précité, § 42.
539 *Ibid.*, § 52.
540 *Ibid.*, § 59.
541 *Ibid.*, §§ 63 et 64.

149. La Cour a jugé qu'en mettant fin anticipativement au mandat de l'autorité nationale de contrôle de la protection des données, à la suite d'un changement de modèle institutionnel décidé par la loi, la Hongrie avait violé ses obligations au titre de l'article 28, § 1, alinéa 2, de la directive 95/46, « laquelle implique l'obligation de respecter la durée du mandat de celle-ci »[542]. Pour la Cour, « s'il était loisible à chaque État membre de mettre fin au mandat d'une autorité de contrôle avant le terme initialement prévu de celui-ci sans respecter les règles et les garanties préétablies à cette fin par la législation applicable, la menace d'une telle cessation anticipée qui planerait alors sur cette autorité (…) pourrait conduire à une forme d'obéissance de celle-ci au pouvoir politique, incompatible avec ladite exigence d'indépendance »[543].

f. Vie privée et communications électroniques

150. Limitations à la confidentialité des communications. La Cour a eu l'occasion de confirmer dans l'affaire *Bonnier*[544] sa jurisprudence bien établie depuis l'affaire *Promusicae*[545] selon laquelle « le droit communautaire, notamment l'article 8, paragraphe 3, de la directive 2004/48[546], lu en combinaison avec l'article 15, paragraphe 1, de la directive 2002/58, ne s'oppose pas à ce que les États membres établissent une obligation de transmission à des personnes privées tierces de données à caractère personnel relatives au trafic pour permettre d'engager, devant les juridictions civiles, des poursuites contre les atteintes au droit d'auteur »[547]. Comme dans l'affaire *Promusicae*, la Cour rappelle que c'est aux États membres d'établir le juste équilibre entre confidentialité des communications d'un côté et protection des droits d'auteur de l'autre. En l'espèce, la Cour a toutefois souligné que la législation suédoise en cause devait être considérée, en principe, comme assurant un juste équilibre puisque qu'elle prévoit que l'injonction judiciaire de communiquer les données d'identification relatives à l'abonné ne peut être ordonnée que si des indices sérieux d'atteinte à un droit de propriété intellectuelle sur une œuvre existent[548]. Cette condition est satisfaisante car elle permet au juge « de pondérer, en fonction des circonstances de chaque espèce et en tenant dûment compte des exigences résultant du principe de proportionnalité, les intérêts opposés en présence »[549].

151. Exception à la confidentialité des communications pour les finalités de facturation. Dans l'affaire *Probst*, la Cour devait préciser les conditions prévues pour la transmission de données de trafic par un fournisseur de services à un tiers, en l'espèce le cessionnaire de ses créances, telle que prévue par l'article 6, §§ 2 et 5, de la Directive 2002/58[550]. Tout d'abord la Cour a considéré que ces dispositions autorisent le traitement de données relatives au trafic, « non

542 C.J.U.E. (gr. ch.), 8 avril 2014, *Commission européenne c. Hongrie*, aff. C-288/12, point 60.
543 *Ibid.*, point 45.
544 C.J.U.E., 19 avril 2012, *Bonnier Audio AB*, aff. C-461/10. Voy. égal. *supra*, n° 70.
545 C.J.U.E. (gr. ch.), 29 janvier 2008, *Productores de Música de España (Promusicae) c. Telefónica de España SAU*, aff. C-275/06. Voy. égal. *supra*, n° 70.
546 Directive 2004/48/CE du Parlement européen et du Conseil du 29 avril 2004 relative au respect des droits de propriété intellectuelle, *J.O.U.E.* L 195 du 2 juin 2004.
547 C.J.U.E., 19 avril 2012, *Bonnier Audio*, précité, point 55. Voy. aussi C.J.C.E., 19 février 2009, *LSG-Gesellschaft c. Tele2 Telecommunication GmbH*, aff. C-557/07, point 29 et C.J.U.E., 29 janvier 2008, *Promusicae*, précité, point 70.
548 C.J.U.E., 19 avril 2012, *Bonnier Audio*, précité, point 58.
549 *Ibid.*, point 59.
550 C.J.U.E., 22 novembre 2012, *Josef Probst c. mr.nexnet GmbH*, aff. C-119/12.

seulement aux fins de l'établissement des factures, mais également aux fins de leur recouvrement »[551]. En deuxième lieu, la Cour a jugé que si l'article 6, §§ 2 et 5, contient une exception à la confidentialité des communications prévue à son article 5, § 1er, en prévoyant la possibilité pour le fournisseur de service de sous-traiter à des tiers les missions de facturation et de recouvrement des créances, le transfert des données de trafic à ces fins devait être restreint aux personnes agissant « sous l'autorité » du fournisseur de services, cette disposition appelant une interprétation stricte[552]. Dans ce cadre, et suivant une lecture combinée des dispositions de la directive 2002/58 et des articles 16 et 17 de la directive 95/46 relatifs au recours à des sous-traitants pour le traitement de données à caractère personnel, la Cour a considéré que l'objectif de l'article 6, § 5, visait bien à ce « qu'une telle externalisation n'affecte pas le niveau de protection des données »[553]. En l'espèce, il revient à la juridiction nationale de vérifier que le contrat conclu entre le fournisseur de services et le cessionnaire de créances comporte les dispositions nécessaires de nature à garantir la licéité du traitement des données de trafic.

g. La protection des données traitées par les institutions de l'Union

152. Articulation des règlements nos 45/2001 et 1049/2001. Dans le prolongement de la jurisprudence *Bavarian Lager*[554], le Tribunal s'est prononcé sur l'équilibre entre la protection de la vie privée et des données à caractère personnel d'un côté, et la transparence administrative de l'autre. Il a notamment précisé dans deux décisions contrastées les obligations de motivation s'appliquant aux institutions refusant l'accès sur le fondement de l'exception prévue à l'article 4, § 1, sous b), du règlement no 1049/2001 et celles s'appliquant au demandeur sollicitant l'accès à des documents couverts par cette exception.

Dans le premier cas, c'est au Parlement européen que le Tribunal a reproché l'absence de motivation pour refuser l'accès à des documents sur la base de l'exception prévue à l'article 4, § 1, sous b). Conformément à une jurisprudence constante selon laquelle « les exceptions à l'accès aux documents doivent être interprétées et appliquées de manière stricte »[555], « une simple affirmation selon laquelle l'accès à certains documents porterait atteinte à la vie privée » n'est pas suffisante[556]. En effet, il incombe à l'institution de procéder à un examen concret et de démontrer dans chaque cas d'espèce, sur la base des informations dont elle dispose, que la divulgation des documents auxquels l'accès est sollicité porterait concrètement et effectivement atteinte à la vie privée des personnes concernées[557], le risque d'atteinte devant être raisonnablement prévisible et non purement hypothétique[558].

Dans le second cas, le Tribunal a confirmé que la demande d'accès à des documents administratifs contenant des données à caractère personnel couverts par l'exception de l'article 4, § 1, sous b),

551 *Ibid.*, point 17.
552 *Ibid.*, point 23.
553 *Ibid.*, point 26.
554 C.J.U.E. (gr. ch.), 29 juin 2010, *Commission c. The Bavarian Lager Co. Ltd*, aff. C-28/08.
555 T.U.E., 28 mars 2012, *Kathleen Egan et Margaret Hackett c. Parlement européen*, aff. T-190/10, point 88.
556 *Ibid.*, point 91.
557 *Ibid.*, points 90, 93, 101.
558 *Ibid.*, point 93.

du règlement nº 1049/20001 devait alors satisfaire les exigences prévues par l'article 8, sous b),[559] du règlement nº 45/2001[560]. Interprétant cette disposition, le Tribunal considère qu'il revient au demandeur destinataire de démontrer dans sa demande la nécessité du transfert, ainsi que le fait qu'il n'existe aucune raison légitime que ce transfert puisse porter atteinte aux intérêts légitimes des personnes concernées, ces deux conditions étant cumulatives[561]. Pour le Tribunal, les demandeurs n'auraient pas suffisamment démontré que le transfert des données qu'ils demandaient était nécessaire en l'espèce.

4. Décision de la Cour européenne des droits de l'homme de Strasbourg

Jean Herveg[562]

153. La notion de vie privée et les informations personnelles. La notion de vie privée est un concept large qui n'est pas susceptible de définition exhaustive et qui recouvre, entre autres choses, les informations relatives à l'identité personnelle comme le nom de la personne, sa photographie ou son intégrité physique et morale. Cette notion s'étend de manière générale aux informations personnelles dont les individus sont légitimement en droit de s'attendre à ce qu'elles ne soient pas publiées sans leur consentement[563]. En principe, elle n'exclut pas les activités de nature professionnelle ou commerciale[564].

154. La protection des données à caractère personnel. La protection des données à caractère personnel, dont les données médicales ne sont pas les moindres, est d'une importance fondamentale à la jouissance du droit au respect de la vie privée d'une personne. Le respect de la confidentialité des données relatives à la santé est un principe vital des systèmes juridiques de tous les États membres de la Convention[565].

155. La protection contre la divulgation d'informations relatives à la santé. Les informations personnelles relatives à un patient appartiennent à sa vie privée. La Cour considère qu'il est primordial d'avoir des règles claires et détaillées en matière de divulgation d'informations médicales confidentielles, et qui offrent des garanties suffisantes contre le risque d'abus et d'arbitraire. La Cour répète à cet égard que la protection des données à caractère personnel, en ce compris les

559 « Les données à caractère personnel ne sont transférées à des destinataires relevant de la législation nationale adoptée en application de la directive 95/46/CE que si a) (….) b) le destinataire démontre la nécessité de leur transfert et s'il n'existe aucune raison de penser que ce transfert pourrait porter atteinte aux intérêts légitimes de la personne concernée ».

560 T.U.E., 13 septembre 2013, *ClientEarth*, précité, point 64.

561 *Ibid.*, point 83.

562 Chargé d'enseignement à la Faculté de droit de Namur (MC Droit de l'Internet), directeur de recherche au CRIDS, avocat au barreau de Bruxelles.

563 Cour eur. D.H., 7 février 2012, arrêt *Axel Springer c. Allemagne*, nº 39954/08, § 83 ; 18 avril 2013, arrêt *Ageyeyvy c. Russie*, nº 7075/10, § 193 ; 19 septembre 2013, arrêt *Von Hannover c. Allemagne (n° 3)*, nº 8772/10, § 41 ; 27 mai 2014, arrêt *de la Flor Cabrera c. Espagne*, nº 10764/09, § 30 ; 12 juin 2014, arrêt *Couderc et Hachette Filipacchi Associés c. France*, nº 40454/07, § 44 ; 9 octobre 2014, arrêt *Konovalova c. Russie*, nº 37873/04, § 39.

564 Cour eur. D.H., 21 janvier 2014, arrêt *Ihsan Ay c. Turquie*, nº 34288/04, § 30 ; 12 juin 2014, arrêt *Fernandez Martinez c. Espagne*, nº 56030/07, § 110 (voy. surtout les opinions dissidentes).

565 Sur l'absence d'une protection légale appropriée, voy. Cour eur. D.H., 29 avril 2014, arrêt *L.H. c. Lettonie*, nº 52019/07, § 56.

informations médicales, est d'une importance fondamentale pour l'exercice du droit au respect de la vie privée et familiale[566].

156. La divulgation, par une institution de soins à l'employeur de la requérante, d'informations à propos de sa grossesse, de son état de santé et de son traitement, représente une ingérence dans son droit au respect de la vie privée. Le droit interne doit indiquer avec une clarté raisonnable l'étendue et la manière d'exercer le pouvoir discrétionnaire conféré aux autorités publiques de manière à garantir aux individus la protection minimale à laquelle ils ont droit dans une société démocratique conformément à la primauté du droit[567].

157. L'obligation d'investiguer et de poursuivre des divulgations non autorisées de données confidentielles. Lorsque des valeurs fondamentales et des aspects essentiels de la vie privée sont en jeu et qu'une dissuasion effective est nécessaire, celle-ci peut être atteinte en premier par des incriminations pénales et leur mise en œuvre effective par le biais d'investigations et de poursuites pénales[568].

158. Le droit d'accès. Une requérante se plaignait de ne pas avoir eu accès aux données collectées à son sujet par les services secrets polonais durant l'ère communiste. La Cour a rappelé que, conformément à sa jurisprudence constante, l'enregistrement de données relatives à la vie privée d'un individu dans un registre secret et sa divulgation tombaient dans le champ de l'article 8, § 1er, et que l'État devait offrir une procédure effective et accessible permettant à une personne d'obtenir un accès complet au fichier créé par les services secrets communistes à son sujet afin de pouvoir contester les allégations relatives à sa collaboration avec ces services[569]. De même, l'État a une obligation positive d'offrir une procédure effective et accessible permettant à une personne d'avoir accès dans un délai raisonnable à l'ensemble des informations recueillies à propos de son père décédé par les anciens services de sécurité communistes, et qui se trouvaient encore en possession des autorités publiques[570].

159. L'accès à des informations permettant d'évaluer les risques pour la santé. L'intégrité physique et psychologique, l'implication des individus dans le choix des traitements médicaux qui leur sont administrés et leur consentement à cet égard, ainsi que leur accès aux informations qui leur permettent d'évaluer les risques de santé auxquels ils sont exposés, tombent dans le champ de l'article 8[571]. Les États ont l'obligation de fournir un accès aux informations essentielles permettant aux individus d'évaluer les risques pour leur santé et pour leur vie[572]. Cette obligation peut aussi comprendre l'obligation de fournir ces informations[573].

566 Cour eur. D.H., 6 juin 2013, arrêt *Avilkina et autres c. Russie*, n° 1585/09, §§ 30, 37 et 45.

567 Cour eur. D.H., 15 avril 2014, arrêt *Radu c. Moldavie*, n° 50073/07, §§ 27 et 28.

568 Cour eur. D.H., 18 avril 2013, arrêt *Ageyeyvy c. Russie*, n° 7075/10, § 196 (dans le cas d'espèce, la Cour a jugé que l'État avait manqué à son obligation d'investiguer et de poursuivre les divulgations non autorisées d'informations confidentielles relatives au statut d'une personne adoptée).

569 Cour eur. D.H., 13 novembre 2012, arrêt *Joanna Szulc c. Pologne*, n° 43932/08, §§ 85-94.

570 Cour eur. D.H., 24 septembre 2013, arrêt *Antoneta Tudor c. Roumanie*, n° 23445/04, § 39.

571 Cour eur. D.H., 23 septembre 2014, arrêt *S.B. c. Roumanie*, n° 24453/04, § 65.

572 Cour eur. D.H., 5 décembre 2013, arrêt *Vilnes et autres c. Norvège*, nos 52806/09 et 22703/10, § 235. Voy. aussi : 15 janvier 2013, arrêt *Csoma c. Roumanie*, n° 8759/05, § 42.

573 Cour eur. D.H., 5 décembre 2013, arrêt *Vilnes et autres c. Norvège*, nos 52806/09 et 22703/10, § 235.

160. La protection de la vie privée et la sécurité nationale. Quand la sécurité nationale est en jeu, les concepts de légalité et de prééminence du droit dans une société démocratique imposent que des mesures affectant des droits fondamentaux de l'homme soient soumises à une certaine forme de procédure contradictoire devant un organe indépendant compétent pour contrôler les raisons de la décision et les preuves pertinentes, le cas échéant avec des limites procédurales appropriées quant à l'usage d'informations classifiées[574].

161. La surveillance secrète des individus. La simple existence d'une législation autorisant les surveillances secrètes constitue une ingérence dans le droit au respect de la vie privée[575]. Ce type de législation doit offrir une protection suffisante contre l'arbitraire et la surveillance indiscriminée[576].

162. La protection des communications. Le droit au respect de la vie privée protège la confidentialité des communications privées, peu importe leur contenu ou leur forme. Ceci signifie que l'article 8 protège la confidentialité de tous les échanges qui peuvent intervenir entre des individus à des fins de communication[577].

163. Les surveillances secrètes des communications. La Cour admet que l'existence de dispositions législatives accordant des pouvoirs de surveillance secrète des communications soit nécessaire dans une société démocratique à la prévention des infractions pénales en matière de lutte contre les formes très complexes de corruption[578]. L'absence de document écrit formalisant le processus décisionnaire ou l'autorisation de procéder à une surveillance secrète est incompatible avec la règle de la primauté du droit, en ce qu'elle confère un pouvoir discrétionnaire illimité et incontrôlé aux autorités d'enquête[579].

164. Les écoutes téléphoniques. Les communications téléphoniques sont comprises dans les notions de « vie privée » et de « correspondance » au sens de l'article 8[580]. Leur interception, leur mémorisation dans un registre secret et la communication de données relatives à la vie privée d'un individu sont des ingérences d'une autorité publique dans l'exercice du droit au respect de la

574 Cour eur. D.H., 28 janvier 2014, décision *I.R. et G.T. c. Royaume-Uni*, n^os^ 14876/12 et 63339/12, § 57. Sur l'usage d'informations confidentielles dans les procédures, voy. les §§ 58 et s.

575 Cour eur. D.H., 23 octobre 2012, arrêt *Hadzhiev c. Bulgarie*, n° 22373/04, § 44 (voy. aussi Cour eur. D.H., 16 octobre 2012, arrêt *Natzev c. Bulgarie*, n° 27079/04 et Cour eur. D.H., 4 décembre 2012, arrêt *Lenev c. Bulgarie*, n° 41452/07, § 144).

576 Cour eur. D.H., 23 octobre 2012, arrêt *Hadzhiev c. Bulgarie*, n° 22373/04, § 45. Voy. aussi Cour eur. D.H., 4 décembre 2012, arrêt *Lenev c. Bulgarie*, n° 41452/07, § 146 ; Cour eur. D.H., 25 juin 2013, arrêt *Acatrinei c. Roumanie*, n° 18540/04, § 58 et Cour eur. D.H., 25 juin 2013, arrêt *Niculescu c. Roumanie*, n° 25333/03, § 99.

577 Cour eur. D.H., 6 décembre 2012, arrêt *Michaud c. France*, n° 12323/11, § 90.

578 Cour eur. D.H., 8 avril 2014, arrêt *Blaj c. Roumanie*, n° 36259/04, § 144.

579 Cour eur. D.H., 2 décembre 2014, arrêt *Taraneks c. Lettonie*, n° 3082/06, § 89.

580 Voy. Cour eur. D.H., 17 janvier 2012, arrêt *Alony Kate c. Espagne*, n° 5612/08, § 73 ; Cour eur. D.H., 31 juillet 2012, arrêt *Draksas c. Lituanie*, n° 36662/04, § 52 ; Cour eur. D.H., 25 juin 2013, Cour eur. D.H., 25 juin 2013, arrêt *Acatrinei c. Roumanie*, n° 18540/04, § 57 ; Cour eur. D.H., 25 juin 2013, arrêt *Niculescu c. Roumanie*, n° 25333/03, § 98 ; Cour eur. D.H., 16 juillet 2013, arrêt *Balteanu c. Roumanie*, n° 142/04, § 41 ; Cour eur. D.H., 19 novembre 2013, arrêt *Ulariu c. Roumanie*, n° 19267/05, § 46 ; Cour eur. D.H., 8 avril 2014, arrêt *Blaj c. Roumanie*, n° 36259/04, § 125 ; Cour eur. D.H., 6 mai 2014, décision *Lachowski c. Pologne*, n° 9208/05, § 72 ; Cour eur. D.H., 2 décembre 2014, arrêt *Taraneks c. Lettonie*, n° 3082/06, § 82.

vie privée[581], ainsi que leur utilisation éventuelle dans le cadre de poursuites pénales[582]. Il importe peu que ce soit au domicile de l'individu ou à son bureau[583].

Conformément à la jurisprudence constante de la Cour en matière de mesures secrètes de surveillance, la loi nationale doit prévoir les protections minimales suivantes afin de prévenir les abus de pouvoir[584] :

- les catégories d'infractions pouvant justifier la mesure de surveillance ;
- les catégories de personnes susceptibles d'avoir leurs téléphones mis sous surveillance ;
- la durée maximale des écoutes téléphoniques ;
- la procédure à suivre pour l'examen, l'utilisation et la conservation des informations collectées ;
- les précautions à prendre pour communiquer ces informations à d'autres personnes ;
- les circonstances dans lesquelles les enregistrements pouvaient ou devaient être effacés ou détruits.

Il faut, de plus, une mesure de protection légale contre l'ingérence arbitraire des autorités publiques dans les droits garantis par l'article 8[585].

L'exigence de prévisibilité de l'interception des communications pour des raisons d'investigations policières ne signifie pas que l'individu doive savoir quand les autorités vont effectivement intercepter ses communications afin qu'il puisse adapter son comportement en conséquence. Toutefois, la loi doit être rédigée en des termes suffisamment clairs pour donner aux citoyens des indications appropriées sur les circonstances et les conditions dans lesquelles les autorités publiques sont autorisées à recourir à cette ingérence secrète et potentiellement dangereuse dans le droit au respect de la vie privée et de la correspondance[586].

La possibilité de mettre sous écoute téléphonique un suspect ne doit pas être restreinte au seul motif que les lignes téléphoniques dont il est titulaire sont également utilisées par d'autres personnes[587]. Lorsque des contacts ont lieu entre un suspect et des tiers, il est loisible aux autorités de mettre sous écoute aussi les lignes téléphoniques appartenant aux tiers concernés, à condition que cette ingérence soit justifiée par un besoin impérieux[588].

---

581 Cour eur. D.H., 17 janvier 2012, arrêt *Alony Kate c. Espagne*, n° 5612/08, § 73 ; Cour eur. D.H., 8 janvier 2013, arrêt *Bucur et Toma c. Roumanie*, n° 40238/02, § 162 ; Cour eur. D.H., 19 novembre 2013, arrêt *Ulariu c. Roumanie*, n° 19267/05, § 46 ; Cour eur. D.H., 8 avril 2014, arrêt *Blaj c. Roumanie*, n° 36259/04, § 125. Voy. aussi Cour eur. D.H., 6 mai 2014, décision *Lachowski c. Pologne*, n° 9208/05, § 72 et Cour eur. D.H., 2 décembre 2014, arrêt *Taraneks c. Lettonie*, n° 3082/06, § 82.

582 Cour eur. D.H., 30 avril 2013, décision *Cariello c. Italie*, n° 14064/07, § 49 ; Cour eur. D.H., 11 juin 2013, décision *D'Auria et Balsamo*, n° 11625/07, § 27 ; Cour eur. D.H., 19 novembre 2013, arrêt *Ulariu c. Roumanie*, n° 19267/05, § 46 ; Cour eur. D.H., 8 avril 2014, arrêt *Blaj c. Roumanie*, n° 36259/04, § 125. Voy. aussi Cour eur. D.H., 6 mai 2014, décision *Lachowski c. Pologne*, n° 9208/05, § 72 et Cour eur. D.H., 2 décembre 2014, arrêt *Taraneks c. Lettonie*, n° 3082/06, § 82.

583 Cour eur. D.H., 27 novembre 2012, arrêt *Savovi c. Bulgarie*, n° 7222/05, § 52.

584 Cour eur. D.H., 2 octobre 2012, arrêt *Sefilyan c. Arménie*, n° 22491/08, § 125 ; Cour eur. D.H., 6 mai 2014, décision *Lachowski c. Pologne*, n° 9208/05, § 85.

585 Voy. Cour eur. D.H., 2 octobre 2012, arrêt *Sefilyan c. Arménie*, n° 22491/08, § 126 ; Cour eur. D.H., 27 novembre 2012, arrêt *Savovi c. Bulgarie*, n° 7222/05, § 55 ; Cour eur. D.H., 16 juillet 2013, arrêt *Balteanu c. Roumanie*, n° 142/04, § 42 ; Cour eur. D.H., 19 novembre 2013, arrêt *Ulariu c. Roumanie*, n° 19267/05, § 49.

586 Cour eur. D.H., 2 octobre 2012, arrêt *Sefilyan c. Arménie*, n° 22491/08, § 123.

587 Cour eur. D.H., 30 avril 2013, décision *Cariello c. Italie*, n° 14064/07, § 63 ; Cour eur. D.H., 11 juin 2013, décision *D'Auria et Balsamo*, n° 11625/07, § 41.

588 Cour eur. D.H., 30 avril 2013, décision *Cariello c. Italie*, n° 14064/07, § 63.

Les droits tirés de l'article 8 par une personne ne sont pas concrètement affectés lorsqu'il s'agit de l'enregistrement des conversations téléphoniques entre des parties tierces auxquelles cette personne n'était pas partie même si ces conversations téléphoniques mentionnent son implication dans des activités criminelles[589].

165. La divulgation du contenu d'écoutes téléphoniques. Comme la procédure à suivre pour les écoutes téléphoniques est sujette à un contrôle judiciaire rigoureux, il est logique que les résultats de celles-ci ne soient pas rendus publics sans un contrôle judiciaire tout aussi strict[590]. La publication dans la presse d'extraits de conversations de nature strictement privée et n'ayant que très peu de rapports avec les accusations portées contre le requérant, voire aucun, ne correspond à aucun besoin social impérieux[591]. Il appartient aux États d'organiser leurs services et de former leur personnel de manière à garantir qu'aucune information confidentielle ou secrète ne soit divulguée[592]. La législation interne doit ménager des garanties appropriées pour empêcher toute communication ou divulgation de données à caractère personnel qui ne serait pas conforme aux garanties prévues à l'article 8. En cas de défaillance de la protection des renseignements confidentiels ou secrets, les autorités doivent ouvrir une enquête effective afin de remédier, dans la mesure du possible, à la situation, notamment en poursuivant les éventuels responsables de l'indiscrétion commise[593]. Le devoir de mener une enquête effective ne saurait être compris comme une obligation de résultat[594].

166. La prise et la conservation de matériel cellulaire ainsi que la réalisation et la conservation de profils ADN. La prise et la conservation de matériel cellulaire ainsi que la réalisation et la conservation de profils ADN constituent des ingérences dans le droit au respect de la vie privée. La loi interne doit offrir des protections appropriées pour prévenir tout usage des données à caractère personnel qui ne serait pas conforme aux garanties de l'article 8. Le besoin de ces protections est d'autant plus grand lorsqu'il s'agit de la protection de données à caractère personnel sujettes à des traitements automatisés, surtout quand ces données sont utilisées à des fins policières. La loi interne doit notamment garantir que ces données soient pertinentes et non excessives au regard des finalités pour lesquelles elles sont conservées, et conservées dans une forme qui permette l'identification des personnes concernées pour une durée qui n'excède pas celle qui est nécessaire pour réaliser la finalité pour laquelle elles sont conservées. La loi interne doit offrir des protections adéquates afin que les données ainsi conservées soient efficacement protégées contre les usages non autorisés et les abus. Ces considérations sont particulièrement valables en ce qui concerne la protection des catégories particulières de données plus sensibles et plus spécialement l'information ADN qui contient la constitution génétique de l'individu qui est de grande importance pour l'individu concerné et sa famille[595].

589 Cour eur. D.H., 4 juin 2013, décision *Fesiuc c. Roumanie*, n° 25497/04, §§ 71 et s. Ceci n'empêche pas que la question soit traitée sous l'angle de l'article 6.

590 Cour eur. D.H., 16 avril 2013, arrêt *Casuneanu c. Roumanie*, n° 22018/10, § 92.

591 *Ibid.*, § 79.

592 *Ibid.*, § 81.

593 *Ibid.*, § 84. Voy. aussi Cour eur. D.H., 10 juin 2014, arrêt *Voicu c. Roumanie*, n° 22015/10, § 86.

594 Cour eur. D.H., 16 avril 2013, arrêt *Casuneanu c. Roumanie*, n° 22018/10, § 86.

595 Cour eur. D.H., 4 juin 2013, décisions *Peruzzo c. Allemagne* et *Martens c. Allemagne*, n^{os} 7841/08 et 57900/12, §§ 33 et 42.

167. L'enregistrement d'images vidéo. L'enregistrement d'images vidéo constitue une ingérence dans la vie privée d'un individu[596].

168. La protection contre les caméras cachées. Une jeune enfant de quatorze ans avait découvert que son beau-père avait installé une caméra dans le but de la filmer lorsqu'elle prenait sa douche dans la salle de bains. Ce dernier a été, *in fine*, acquitté par les juridictions suédoises. Devant la Cour, la jeune fille s'est plainte d'une violation de son droit au respect de la vie privée. La Chambre de la 5e section de la Cour a rappelé que les États devaient posséder et mettre réellement en œuvre un cadre juridique approprié qui offre une protection contre les actes de violence commis par des particuliers[597] et que si le recours au droit pénal n'est pas nécessairement l'unique solution, la dissuasion effective contre des actes graves à propos de valeurs fondamentales et d'aspects essentiels de la vie privée requiert des dispositions efficaces de droit pénal[598].

169. En ce qui concerne des enfants, la Grande Chambre a indiqué que les dispositifs mis en place par l'État pour les protéger contre des actes de violence devaient être efficaces et inclure des mesures raisonnables visant à empêcher les mauvais traitements dont les autorités avaient ou auraient dû avoir connaissance, ainsi qu'une prévention efficace visant à mettre les enfants à l'abri de formes aussi graves d'atteinte à leur intégrité. Ces mesures doivent viser à garantir le respect de la dignité humaine et la protection de l'intérêt supérieur de l'enfant. S'agissant plus spécifiquement d'actes aussi graves que le viol et les abus sexuels sur des enfants qui mettent en jeu des valeurs fondamentales et des aspects essentiels de la vie privée, il appartient aux États de se doter de dispositions pénales efficaces. Concernant des actes d'une telle gravité, l'obligation positive qui incombe à l'État peut s'étendre aux questions touchant à l'effectivité d'une enquête pénale et à la possibilité d'obtenir redressement et réparation, même s'il n'existe pas un droit absolu à obtenir l'ouverture de poursuites contre une personne donnée, ou la condamnation de celle-ci, lorsqu'il n'y a pas eu de défaillances blâmables dans les efforts déployés pour obliger les auteurs d'infractions pénales à rendre des comptes.

170. Pour les actes qui pourraient passer pour présenter une gravité moins élevée, une protection pratique et efficace suppose l'existence de recours permettant d'identifier l'auteur des actes incriminés et de le traduire en justice. Pour ce qui est plus généralement des actes interindividuels de moindre gravité, l'obligation qui incombe à l'État de mettre en place et d'appliquer concrètement un cadre juridique adapté n'implique pas toujours l'adoption de dispositions pénales visant les différents actes pouvant être en cause. Le cadre juridique peut aussi consister en des recours civils aptes à fournir une protection suffisante[599].

171. Dans l'affaire *E.S. c. Suède*, la Chambre de la 5e section de la Cour avait souligné le fait qu'une vigilance croissante était nécessaire pour protéger la vie privée en présence de nouvelles techno-

596 Sur l'enregistrement d'images vidéo par des détectives privés et leur utilisation ultérieure à des fins probatoires : Cour eur. D.H., 19 septembre 2013, arrêt *Von Hannover c. Allemagne (n° 3)*, n° 8772/10, §§ 30 et s.

597 Cour eur. D.H., 21 juin 2012, arrêt *E.S. c. Suède*, n° 5786/08, § 58. Ce point fut repris par l'arrêt rendu en Grande Chambre le 12 novembre 2013, *Soderman c. Suède*, n° 5786/08, § 80.

598 Cour eur. D.H., 21 juin 2012, arrêt *E.S. c. Suède*, n° 5786/08, § 58.

599 Cour eur. D.H. (gr. ch.), 12 novembre 2013, arrêt *Soderman c. Suède*, n° 5786/08, §§ 81-85. La Cour a noté 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.

logies de la communication qui rendent possible l'enregistrement et la diffusion de données à caractère personnel[600].

172. Les archives sur internet. Le risque de préjudice posé par le contenu et les communications sur l'internet à l'exercice et à la jouissance des droits et libertés, en particulier le droit au respect de la vie privée, est plus élevé que ceux posés par la presse traditionnelle. En conséquence, les règles relatives à la communication d'informations peuvent différer entre les médias imprimés et l'internet[601].

173. Les fichiers d'enregistrement des immatriculations. La Cour a été saisie d'une affaire dans laquelle le permis du requérant lui avait été dérobé. Les voleurs ont ensuite utilisé ce permis pour enregistrer 1.737 voitures dans le registre des immatriculations. La situation a causé de très nombreux désagréments au requérant et les juridictions internes n'ont jamais accepté d'y remédier de façon suffisante. La Cour a d'abord considéré que le défaut d'invalider le permis de conduire du requérant dès que son vol avait été déclaré (ce qui a rendu possible l'abus de l'identité du requérant par des tiers), constituait une ingérence dans le droit du requérant au respect de sa vie privée. La Cour a ensuite jugé qu'il n'était pas nécessaire de se pencher sur la question de savoir si le requérant avait pris les mesures appropriées par rapport aux enregistrements abusifs de véhicules en son nom. Elle a simplement considéré que, dès le moment où le requérant avait déclaré le vol de son permis de conduire, les autorités publiques néerlandaises ne pouvaient plus prétendre ignorer que le détenteur du permis n'était pas le requérant[602].

174. La conservation de données à caractère personnel par la police. Dans une affaire relative à des données conservées par la police autrichienne sur des poursuites engagées contre des hommes majeurs pour avoir eu des relations sexuelles consenties avec d'autres hommes, la Cour a rappelé que la conservation, par des autorités publiques, d'informations relatives à la vie privée d'un individu constitue une ingérence au sens de l'article 8[603]. Le droit national doit fournir des garanties appropriées pour prévenir tout usage de ces données à caractère personnel qui ne serait pas conforme avec les garanties de l'article 8. Aux yeux de la Cour, le besoin de ces garanties est encore plus grand quand la protection des données à caractère personnel soumises à des traitements automatisés est concernée, surtout quand ces données sont utilisées à des fins policières. Le droit national doit, en particulier, assurer que ces données sont pertinentes et non excessives au regard des finalités pour lesquelles elles sont conservées et qu'elles ne sont pas gardées sous une forme qui permette l'identification des personnes concernées plus longtemps que ce qui est requis pour la finalité pour laquelle ces données sont conservées. Le droit national doit aussi offrir des garanties adéquates pour assurer que les données à caractère personnel conservées soient efficacement protégées contre les usages abusifs[604].

600 Cour eur. D.H., 21 juin 2012, arrêt *E.S. c. Suède*, n° 5786/08, § 71.

601 Cour eur. D.H., 16 juillet 2013, arrêt *Wegrzynowski et Smolczewski c. Pologne*, n° 33846/07, § 58. Voy. sur la question de la responsabilité pour des propos diffamatoires tenus sur un portail d'actualités sur internet, l'arrêt du 10 octobre 2013, *Delfi AS c. Estonie*, n° 64569/09, renvoyé devant la Grande Chambre qui s'est prononcée dans un arrêt du 16 juin 2015.

602 Cour eur. D.H., 14 février 2012, arrêt *Romet c. Les Pays-Bas*, n° 7094/06, §§ 37 et s.

603 Cour eur. D.H., 25 mars 2014, décision *F.J. et E.B. c. Autriche*, n^{os} 2362/08 et 26271/08, §§ 71-72.

604 Cour eur. D.H., 25 mars 2014, décision *F.J. et E.B. c. Autriche*, n^{os} 2362/08 et 26271/08, § 73. Sur l'inscription d'une personne dans le STIC français (le système de traitement des infractions constatées), voy. Cour eur. D.H., 18 septembre 2014, arrêt *Brunet c. France*, n° 21010/10.

175. Les perquisitions et saisies de données informatiques. La perquisition et la saisie des fichiers informatiques d'un bureau d'avocats constituent une ingérence dans le droit au respect de la correspondance[605]. Le droit interne et la pratique doivent fournir des protections adéquates et effectives contre les abus et l'arbitraire. En particulier, il faut vérifier si la perquisition a été autorisée par un juge et qu'elle est justifiée par des motifs raisonnables.

L'objet de la perquisition doit être raisonnablement délimité. Lorsqu'il s'agit de perquisitionner un bureau d'avocats, la perquisition doit être réalisée en présence d'un observateur indépendant afin que les éléments protégés par le secret professionnel ne soient pas emportés[606]. Concrètement, la police ne devrait pouvoir consulter et saisir que les fichiers informatiques en relation avec les raisons pour lesquelles la perquisition a été autorisée et non pas tous les fichiers informatiques sans distinction aucune.

En matière de contrôle fiscal, lorsque plusieurs entreprises partagent un même serveur sans que leurs archives ne soient clairement séparées, il est raisonnable de considérer que les autorités fiscales n'ont pas à s'en remettre aux indications des personnes contrôlées pour trouver les informations sur un serveur mais qu'elles doivent pouvoir avoir accès à toutes les données reprises sur le serveur afin de procéder elles-mêmes au tri des données[607].

La perquisition d'un club informatique ainsi que la saisie et la conservation d'ordinateurs contenant prétendument des informations personnelles constituent des ingérences dans le droit au respect de la vie privée du gérant du club et de son épouse qui l'assistait et le remplaçait quand il s'absentait tout en fournissant des services de dactylographie au public via l'usage des ordinateurs du club. La Cour peut admettre, dans certaines situations, que l'absence d'un mandat judiciaire préalable soit contrebalancée par l'existence d'un contrôle judiciaire rétrospectif[608].

176. La collecte et la conservation de données issues du casier judiciaire. Les données relatives à la mise en garde de la requérante et contenues dans les fichiers de la police sont des données à caractère personnel et des données sensibles. Ils font partie, en outre, de son casier judiciaire. La Cour considère qu'il est essentiel, dans le contexte de l'enregistrement et de la divulgation de données du casier judiciaire comme pour les écoutes téléphoniques, les surveillances secrètes et la collecte secrète d'informations, d'avoir des règles claires et détaillées qui gouvernent la portée et la mise en œuvre des mesures. Il faut aussi un minimum de règles concernant, notamment, la durée, la conservation, l'utilisation, l'accès par des tiers, les procédures de destruction, afin de fournir des garanties suffisantes contre le risque d'abus et d'arbitraire. Il y a de nombreuses étapes au cours desquelles des problèmes de protection de données peuvent surgir au regard de l'article 8, en ce compris lors de la collecte, la conservation, l'utilisation et la communication des données. À chaque étape, des protections adéquates et appropriées doivent exister et qui reflètent les principes élaborés dans les instruments applicables en matière de protection des

605 Cour eur. D.H., 3 juillet 2012, arrêt *Robathin c. Autriche*, n° 30457/06, § 39.

606 *Ibid.*, § 44.

607 En ce sens, Cour eur. D.H., 14 mars 2013, arrêt *Bernh Larsen Holding AS et autres c. Norvège*, n° 24117/08, § 132.

608 Cour eur. D.H., 30 septembre 2014, arrêt *Prezhdarovi c. Bulgarie*, n° 8429/05, §§ 41 et 46. Voy. aussi à propos de l'inspection opérée dans des locaux professionnels d'une société, Cour eur. D.H., 2 octobre 2014, arrêt *Delta Pekarny A.S. c. République tchèque*, n° 97/11.

données et empêcher l'arbitraire et les ingérences disproportionnées dans les droits garantis par l'article 8.

La collecte indiscriminée et illimitée de données dans le casier judiciaire peut difficilement être conforme avec les exigences de l'article 8 en l'absence de règles claires et détaillées décrivant, notamment, les situations dans lesquelles des données peuvent être collectées, la durée de leur conservation, l'usage qui peut en être fait et les circonstances dans lesquelles elles peuvent être détruites.

L'obligation de garantir le respect de la vie privée qui pèse sur les autorités responsables de la conservation et de la divulgation des données du casier judiciaire est particulièrement importante considérant la nature des données détenues et les conséquences potentiellement dévastatrices de leur divulgation. Dans la plupart des cas, un certificat défavorable du casier judiciaire aura un effet dévastateur sur les chances d'une personne qui souhaite postuler à un emploi qui requiert sa production. C'est au regard de cet effet que doit être évaluée la légalité des mesures en matière de conservation et de divulgation des données du casier judiciaire[609].

177. La protection des communications en prison. L'article 8 ne garantit pas aux prisonniers le droit de téléphoner, en particulier quand il leur est loisible de correspondre par écrit. Lorsque la prison leur offre la possibilité de téléphoner, il peut y avoir des contraintes légitimes liées, par exemple, au fait que les équipements sont partagés avec les autres prisonniers ou à la nécessité de prévenir les désordres et les infractions[610].

La présence d'un gardien lors des communications téléphoniques et l'enregistrement des numéros composés depuis la prison constituent des ingérences dans le droit des détenus au respect de leur vie privée mais justifiées dans la mesure où cette surveillance est moins intrusive que les écoutes téléphoniques, et que le détenu est averti de cette surveillance[611].

Lorsqu'un courrier électronique est envoyé à la boîte à message générale de la prison mais avec l'indication qu'il est destiné à un détenu déterminé et qu'il est demandé de le lui communiquer, le détenu peut s'attendre à ce que cette correspondance soit protégée par l'article 8. Il n'y a pas d'obligation positive à charge de l'État d'autoriser l'usage des e-mails. Le refus de communiquer l'e-mail au détenu n'est pas non plus une mesure disproportionnée dès lors que son expéditeur avait été prévenu de la non-communication du message et avait été requis d'utiliser les moyens de communication autorisés par la législation nationale[612].

178. Les analyses volontaires d'ADN à des fins d'identification de cadavres. Lorsque des personnes ont volontairement donné des échantillons ADN à des fins d'identification de cadavres après avoir été informées des finalités poursuivies et en l'absence de toute indication permettant

609 Cour eur. D.H., 13 novembre 2012, arrêt *M.M. c. Royaume-Uni*, n° 24029/07, §§ 188, 195, 200-201. Voy. aussi Cour eur. D.H., 24 juin 2014, décision *E.B. c. Autriche*, n° 27783/09, § 29. À propos de l'inscription au FIJAIS (fichier judiciaire national des auteurs d'infractions sexuelles en France), voy. Cour eur. D.H., 16 septembre 2014, décision *J.P.D. c. France*, n° 55432/10.

610 Cour eur. D.H., 2 octobre 2012, décision *Daniliuc c. Roumanie*, n° 7262/06, § 68. Sur la contrainte linguistique imposée aux détenus kurdes, voy. Cour eur. D.H., 22 avril 2014, arrêt *Nusret Kaya et autres c. Turquie*, n^{os} 43750/06, 43752/06, 32054/08, 37753/08 et 60915/08, §§ 36 et 42.

611 Cour eur. D.H., 25 juin 2013, arrêt *Niculescu c. Roumanie*, n° 25333/03, § 92.

612 Cour eur. D.H., 10 septembre 2013, arrêt *Helander c. Finlande*, n° 10410/10, §§ 48, 53-54.

de penser que ces échantillons auraient été utilisés à d'autres fins, il n'y a pas d'ingérence dans le droit au respect de la vie privée de ces volontaires[613].

179. Registre de faillis. L'Italie a encore fait l'objet d'une série de condamnations pour sa législation en matière d'inscription dans le registre des faillis compte tenu de la nature automatique de l'inscription, de l'absence de toute évaluation et de tout contrôle juridictionnel sur l'application des incapacités et du laps de temps prévu pour l'obtention d'une réhabilitation (soit cinq ans après la clôture de la procédure de faillite)[614].

5. Usage des technologies de l'information et de la communication dans les relations de travail et droit au respect de la vie privée

Karen Rosier[615]

180. Introduction. Les questions posées par l'usage de nouvelles technologies dans les relations de travail continuent de nourrir des litiges. La plupart se situent dans le cadre d'une rupture de contrat. Si l'on retrouve des décisions relatives à des contrôles effectués par l'employeur, ayant trait à un contrôle de la boîte mail, de l'usage d'internet ou de fichiers stockés dans un ordinateur qui aboutissent à un licenciement, on voit toutefois poindre de nouvelles pratiques favorisées par la généralisation de nouveaux équipements tels des smartphones. Ainsi, plusieurs décisions traitent d'enregistrements de conversations soit audio, soit audio et vidéo, réalisés à l'insu d'une personne dans le seul but de se constituer une preuve.

181. La gageure de la problématique reste la même. Concilier les intérêts opposés que sont le droit au respect de la vie privée et le droit à l'exercice d'un certain contrôle, expression de l'autorité patronale, et cela dans un contexte où plusieurs législations sont parfois à appliquer cumulativement à une même mesure de contrôle. Nous avons relevé, dans la précédente chronique[616], une tendance de la jurisprudence à donner une place prépondérante à l'article 8 de la CEDH dans l'analyse des solutions aux litiges, nonobstant l'existence de règles parfois plus particulières et qui concrétisent les principes de droit au respect de la vie privée dans des cas spécifiques, tel le secret des communications électroniques.

182. Cette tendance se maintient et on note quelques applications intéressantes du critère des attentes raisonnables pour apprécier si un droit au respect de la vie privée peut être invoqué dans une situation donnée. Ce critère est appliqué tant lorsqu'il s'agit de déterminer si un enregistrement audio ou celui d'une communication téléphonique, réalisé à l'insu de l'interlocuteur, constitue une violation du droit au respect de la vie privée que lorsqu'il s'agit, dans le cadre d'autres contextes de licenciement liés à la publication de messages sur Facebook par le travailleur, de déterminer si et quand le travailleur perd le droit d'invoquer le caractère privé de ces communications pour s'opposer à leur utilisation comme motif de licenciement.

613 Cour eur. D.H., 23 septembre 2014, décision Cakicisoy et autres c. Chypre, n° 6523/12, §§ 50-51.

614 Cour eur. D.H., 18 décembre 2012, arrêt *Salvatore Coppola et autres c. Italie*, n^{os} 5179/05, 14611/05, 29701/06, 9041/05 et 8239/05, §§ 36 et s. ; Cour eur. D.H., 5 mars 2013, arrêt *De Carolis c. Italie*, n° 33359/05.

615 Maître de conférences à l'Université de Namur, checheuse senior au CRIDS (UNamur), avocate.

616 K. Rosier, « Usage des technologies de l'information et de la communication dans les relations de travail et droit au respect de la vie privée, Chronique de jurisprudence en droit des technologies et de l'information (2009-2011) », *R.D.T.I.*, 2012, pp. 127-145.

6. Des actes constitutifs d'atteintes à la vie privée des travailleurs

a. Le point sur la jurisprudence rendue en matière de communications électroniques

183. Cadre légal. La prise de connaissance d'une communication électronique par des tiers à cette communication reste toujours à l'heure actuelle régie par un cadre légal complexe. Outre le droit au respect de la vie privée (articles 8 de la CEDH et 22 de la Constitution), s'appliquent les dispositions relatives au secret des communications électroniques (principalement les articles 124 et suivants de la loi du 13 juin 2005 relative aux communications électroniques et l'article 314*bis* du Code pénal) mais aussi celles qui régissent le traitement de données à caractère personnel (loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel). La Convention collective de travail n° 81 relative à la protection de la vie privée des travailleurs à l'égard du contrôle des données de communications électroniques reste également d'actualité. À signaler toutefois, la recommandation n° 08/2012 de la Commission de la Protection de la Vie Privée[617] qui analyse la problématique du contrôle des e-mails et des connexions internet sur le lieu du travail et livre une interprétation nouvelle de cette réglementation dans laquelle la CCT n° 81 est d'ailleurs mise en avant. La Commission estime que les directives issues de la CCT n° 81 permettent de comprendre ce qui correspond à un exercice normal de l'autorité patronale en matière de surveillance des e-mails et de connexions internet[618].

§ 1. Violation du droit au respect de la vie privée : variations autour du critère des attentes raisonnables

184. L'enregistrement d'une conversation téléphonique. Dans un arrêt du 8 janvier 2014[619], la Cour de cassation s'est prononcée sur la question de la régularité de la preuve obtenue via un enregistrement de télécommunication réalisé à l'insu d'un des interlocuteurs.

Elle énonce tout d'abord que l'interdiction de prendre connaissance et d'enregistrer une télécommunication ne s'applique pas à la personne qui, partie prenante à cette communication, enregistre son contenu avec l'accord ou même à l'insu de son interlocuteur.

La Cour considère, par ailleurs, qu'un tel enregistrement ne viole ni les articles 6 et 8 de la CEDH ni l'article 314*bis* du Code pénal dès lors qu'il s'agit d'une utilisation d'un tel enregistrement à des fins probatoires par la personne qui, apprenant l'existence d'un crime ou d'un délit, s'acquitte de l'obligation d'en donner avis au procureur du Roi. L'arrêt laisse donc penser que l'appréciation de l'absence de violation de ces dispositions se justifie par rapport à la finalité d'utilisation de l'enregistrement. Rappelons que, dans un arrêt rendu le 9 novembre 2008[620], la Cour de cassation

617 Commission de la Protection de la Vie Privée, recommandation n° 2012/08 d'initiative relative au contrôle de l'employeur quant à l'utilisation des outils de communication électronique sur le lieu de travail, 2 mai 2012, www.privacycommission.be.

618 Commission de la Protection de la Vie Privée, Rapport juridique en vue d'adresser aux partenaires sociaux, aux organes de concertation qu'ils constituent et de manière générale à tous les employeurs et travailleurs, des recommandations visant à concilier les prérogatives de l'employeur avec la protection des données à caractère personnel des travailleurs ou de tiers lors de l'utilisation, de la surveillance et du contrôle des outils informatiques de communication électronique dans le cadre de la relation de travail, 2012, www.privacycommission.be, p. 24.

619 Cass. (2e ch.), 8 janvier 2014, R.G. n° P.13.1935.F.

620 Cass., 9 septembre 2008, R.G. n° P.08.0276.N. Pour un commentaire détaillé de cet arrêt, voy. F. Raepsaet, « Les attentes raisonnables en matière de vie privée », *J.T.*, 2011, n° 1094, pp. 145 et s.

avait considéré que si le seul fait d'enregistrer une conversation à laquelle on participe soi-même n'est pas illicite du fait qu'il est réalisé à l'insu des autres participants, cet acte peut constituer une violation de l'article 8 de la CEDH. La Cour ajoutait qu'il revenait au juge d'apprécier si l'usage de cet enregistrement était autorisé, il devait inclure dans son jugement le critère des attentes raisonnables de la personne concernée en matière de respect de sa vie privée. Dans l'arrêt du 8 janvier 2014, ce critère des attentes raisonnables n'est donc pas repris pour apprécier l'existence d'une violation de l'article 8 CEDH. L'arrêt étant assez succinct, on ne connaît d'ailleurs pas les circonstances exactes de cet enregistrement.

Le critère des attentes raisonnables est en revanche pris en compte par le président du tribunal du travail de Bruges dans un jugement du 10 décembre 2013[621]. Confrontés à une situation de discrimination à l'embauche liée au handicap, les parents du candidat malheureux avaient réalisé un enregistrement d'une conversation téléphonique avec l'administratrice déléguée de l'employeur concerné, enregistrement qui permettait d'établir que le refus de contrat de travail était lié au handicap, une malformation congénitale des mains, dont souffrait leur fils.

Le président du tribunal va considérer que l'administratrice en question ne pouvait avoir des attentes raisonnables concernant le fait que la conversation ne serait pas enregistrée dès lors qu'elle savait ou devait savoir que ces parents et leur enfant se sentaient victimes d'une discrimination. Il va estimer que : « L'enregistrement d'une conversation avec le responsable de la société, ainsi que le traitement informatique de cet entretien par le Centre pour l'égalité des chances, sont, même si ce responsable n'avait pas au préalable donné son accord à cet enregistrement, justifiés eu égard au caractère non confidentiel de l'entretien, à son contenu purement objectif, au fait qu'il n'y avait pas de lien intime entre les personnes mêlées à la conversation, et aussi au sujet de l'entretien ».

185. Données de communications GSM. C'est à nouveau le critère des attentes raisonnables qui est mis en exergue dans un arrêt de la cour du travail de Gand du 12 mai 2014[622]. Un travailleur faisait grief à son employeur de produire des relevés d'appels téléphoniques mettant en évidence l'utilisation du GSM de l'entreprise par le travailleur pour appeler des lignes astrologiques, au motif que cela serait contraire à son droit au respect de la vie privée. La cour parvient à la conclusion contraire en considérant que l'employeur reçoit ou peut recevoir ces données de communications en sa qualité d'abonné et que le travailleur pouvait raisonnablement s'attendre à ce que son employeur effectue un contrôle des factures qu'il reçoit. En l'absence de convention particulière concernant l'usage de ce GSM, il revient à l'employeur, sur la base de son pouvoir d'autorité, de déterminer quel usage du GSM est acceptable. Incidemment, on notera que la cour va juger qu'utiliser le GSM de l'entreprise pour appeler principalement des numéros surtaxés tels des lignes astrologiques est constitutif d'une faute grave.

186. Consultations de courriers électroniques dans la boîte mail de l'employeur. Dans un arrêt du 7 février 2013[623], la cour du travail de Bruxelles a eu à connaître d'un litige portant sur

621 Prés. Trib. trav. Bruges, 10 décembre 2013, *Chron. D.S.*, 2014, liv. 7, p. 339 ; *T.G.R.-T.W.V.R.*, 2014, liv. 2, p. 156.

622 C. trav. Gand (div. Gand, 2e ch.), 12 mai 2014, *J.T.T.*, 2014, p. 320 ; *R.W.*, 2014-2015, liv. 40, p. 1586.

623 C. trav. Bruxelles (2e ch.), 7 février 2013, R.G. n° 2012/AB/1115, www.juridat.be ; *J.T.*, 2013, liv. 6516, note D. Mougenot ; *Ors.*, 2013 (reflet B. Paternostre), liv. 4, p. 25 ; *Chron. D.S.*, 2013, liv. 2, p. 106, note O. Rijckaert. Cette décision fait l'objet d'un pourvoi.

la validité d'un licenciement pour motif grave dont la preuve était rapportée par des courriers électroniques d'un travailleur. Ceux-ci avaient été portés à la connaissance de l'employeur par l'assistante du travailleur en question, qui avait accédé en son absence, à son insu et sans son autorisation, à sa boîte mail. Les courriers litigieux révélaient l'existence d'une activité parallèle exercée durant le temps de travail et au moyen des outils de communications de l'employeur. Les informations révélant cette activité étaient toutefois contenues dans des e-mails à caractère privé ce qui était ressorti tant de la qualité des destinataires (des membres de la famille du travailleur) que du ton familier utilisé. La cour se rallie à la décision du premier juge qui avait considéré que ces courriers électroniques relèvent de la sphère privée du travailleur et que le contrôle est intervenu en violation du droit au respect de la vie privée. Elle a considéré qu'en allant consulter les courriels envoyés par ce travailleur, sans l'accord de celui-ci, sans lui en communiquer les finalités et en l'absence de règles déterminées portées à la connaissance dudit travailleur, autorisant la société à effectuer une telle consultation, la société appelante a violé le droit au respect de la vie du travailleur.

§ 2. Secret des communications électroniques

187. Portée de l'article 124 de la loi du 13 juin 2005 relative aux communications électroniques[624]**.** Dans l'arrêt précité du 7 février 2013, la cour du travail de Bruxelles se penche sur le caractère intentionnel ou fortuit de la prise de connaissance de courriers électroniques par un tiers. Elle rappelle que la charge de la preuve de ce caractère éventuellement fortuit de la prise de connaissance incombe à celui qui s'en prévaut, en l'occurrence l'employeur. La cour indique tout d'abord qu'il est indifférent que la personne qui a pris connaissance des courriers ne soit pas l'employeur directement mais une assistante. Il s'agit d'une préposée de l'employeur qui agissait sinon selon les instructions de l'employeur, à tout le moins avec son autorisation. Lors d'un conseil d'entreprise, il avait en effet été communiqué que si des tiers accédaient à des boîtes mails, il s'agissait souvent des assistantes et que cela ne visait que les mails professionnels. En l'espèce, la cour conclura à l'absence de caractère fortuit de la prise sur la base des considérations suivantes : les messages étaient manifestement personnels, ne pouvaient être pris pour des messages urgents appelant une réaction en l'absence du travailleur dès lors qu'ils se trouvaient dans la boîte d'envoi et étaient antérieurs à la période de congés du travailleur. Elle conclut à une violation de l'article 124 de la loi du 13 juin 2005.

188. Enregistrement de conversations téléphoniques. Saisie d'une plainte émanant d'un travailleur concernant l'enregistrement de conversations téléphoniques entre les membres du

624 Cette disposition prévoit que :
« S'il n'y est pas autorisé par toutes les personnes directement ou indirectement concernées, nul ne peut :
1° prendre intentionnellement connaissance de l'existence d'une information de toute nature transmise par voie de communication électronique et qui ne lui est pas destinée personnellement ;
2° identifier intentionnellement les personnes concernées par la transmission de l'information et son contenu ;
3° sans préjudice de l'application des articles 122 et 123 prendre connaissance intentionnellement de données en matière de communications électroniques et relatives à une autre personne ;
4° modifier, supprimer, révéler, stocker ou faire un usage quelconque de l'information, de l'identification ou des données obtenues intentionnellement ou non ».

personnel d'un magasin et de nouveaux clients[625], la Commission a estimé que cet enregistrement ne violait ni l'article 124 de la loi du 13 juin 2005 sur les communications électroniques ni l'article 314*bis* du Code pénal[626]. Ces deux dispositions ont trait au secret des communications électroniques et font obstacle à l'enregistrement pour prise de connaissance d'un entretien téléphonique sans l'accord de toutes les personnes parties à la communication. La Commission a constaté que l'enregistrement de la conversation n'intervenait qu'à la condition que le client y ait préalablement consenti.

Pour ce qui est du travailleur, la Commission considère que « les articles 2, 3 et 17, 2°, de la loi sur le contrat de travail constituent en soi une autorisation légale pour déroger aux dispositions d'interdiction de l'article 314*bis* du Code pénal et l'article 124 de la loi du 13 juin 2005 et que par conséquent l'employeur est autorisé, sous certaines conditions, à prendre connaissance, par exemple, du contenu des conversations téléphoniques entre ses travailleurs et des tiers ». Autrement dit, la Commission est d'avis que les dispositions de la loi sur le contrat de travail qui consacrent le pouvoir d'autorité de l'employeur sur le travailleur serait une loi qui permet les actes prohibés par les dispositions précitées au sens de l'article 125, 1°, de la loi sur les communications électroniques[627]. La seule exigence que semble retenir la Commission est celle du respect de la loi du 8 décembre 1992.

Cette position est nouvelle dans le chef de la Commission et semble s'inscrire dans la droite ligne de la recommandation qu'elle a émise en 2012 en matière de cybersurveillance[628]. La Commission se fonde toutefois sur la position minoritaire de la jurisprudence et de la doctrine. Notons encore que la Commission n'évoque pas l'article 128, § 2, de la loi du 13 juin 2005 qui règle spécifiquement l'enregistrement de conversations téléphoniques avec la clientèle dans les *calls centers*[629].

---

625 Commission de la Protection de la Vie Privée, avis n° 18/2013 du 5 juin 2013 formulé suite à une plainte contre une plate-forme de garantie de qualité visant à enregistrer des conversations téléphoniques entre des travailleurs et des clients potentiels de l'employeur, www.privacycommission.be.

626 L'article 314*bis* du Code pénal prévoit que :
« § 1. Sera puni d'un emprisonnement de six mois à un an et d'une amende de deux cents [euros] à dix mille [euros] ou d'une de ces peines seulement, quiconque :
1° soit, intentionnellement, à l'aide d'un appareil quelconque, écoute ou fait écouter, prend connaissance ou fait prendre connaissance, enregistre ou fait enregistrer, pendant leur transmission, des communications ou des télécommunications privées, auxquelles il ne prend pas part, sans le consentement de tous les participants à ces communications ou télécommunications ;
2° soit, avec l'intention de commettre une des infractions mentionnées ci-dessus, installe ou fait installer un appareil quelconque (…) ».

627 Aux termes de l'article 125, § 1er : « Les dispositions de l'article 124 de la présente loi et les articles 259*bis* et 314*bis* du Code pénal ne sont pas applicables : (…) 1° lorsque la loi permet ou impose l'accomplissement des actes visés ».

628 Commission de la Protection de la Vie Privée, Rapport juridique établi à l'initiative de la Commission de la protection de la vie privée en rapport avec la recommandation n° 08/2012 du 2 mai 2012 relative au contrôle de l'employeur quant à l'utilisation des outils de communication électronique sur le lieu de travail, pp. 12 à 14, www.privacycommission.be.

629 Cet article 128, § 2, stipule que : « Par dérogation aux articles 259*bis* et 314*bis* du Code pénal, la prise de connaissance et l'enregistrement de communications électroniques et des données de trafic, qui visent uniquement à contrôler la qualité du service dans les call centers sont autorisés, à condition que les personnes qui travaillent dans le call center soient informées au préalable et, sans préjudice de l'application de la loi du 8 décembre 1992 relative à la protection de la vie privée, de la possibilité de prise de connaissance et d'enregistrement, du but précis de cette opération et de la durée de conservation de la communication et des données enregistrées. Ces données peuvent être conservées maximum un mois ».

Concernant le respect de la loi du 8 décembre 1992, la Commission estime que n'est pas disproportionné le traitement impliqué par un système par lequel il s'agit de procéder au suivi périodique de la qualité de la relation du service à la clientèle en vue de proposer, sur la base de ce suivi, un coaching et une formation opérationnels adaptés, sans que des sanctions ou des récompenses ne soient liées à ce contrôle de la qualité pour les employés.

§ 3. Application de la CCT n° 81

189. Champ d'application de la CCT n° 81. Dans un arrêt du 26 novembre 2014, la cour du travail de Liège, division de Neufchâteau[630], a écarté l'application de la CCT n° 81 pour le contrôle de fichiers se trouvant sur le disque dur d'un PC. La cour rappelle que la CCT n° 81 vise le contrôle de données de communications électroniques et n'établit le cadre au contrôle pouvant être opéré par l'employeur que pour les seules données de communications électroniques.

Une des particularités de ce litige était toutefois qu'au cours du contrôle destiné initialement à vérifier quelle pouvait être la cause de la disparition de données de l'entreprise, l'employeur avait découvert que le travailleur à l'origine de la perte de données passait de nombreuses heures sur internet à consulter des sites étrangers à ses activités professionnelles plutôt qu'à l'exécution de ses tâches. Le travailleur ayant laissé son ordinateur allumé, l'employeur avait pu accéder au contenu de l'ordinateur. Il est apparu que le travailleur faisait tourner via une clé USB qui était connectée au PC un programme CCleaner destiné à effacer les données de navigation sur internet. L'employeur demandera à un informaticien d'installer un logiciel de contrôle de l'activité sur le PC pendant une journée de travail. Les données ainsi collectées vont incidemment faire apparaître que le travailleur passe l'essentiel de sa journée de travail à des activités privées.

La cour va considérer que l'employeur n'avait pas à respecter la CCT n° 81 vu que le contrôle était destiné à vérifier l'impact de l'usage du programme sur le PC. Le fait qu'incidemment, l'employeur ait pris connaissance de données de communications électroniques (données de consultation de sites internet) n'implique pas une violation de la CCT, selon la cour.

b. Le point sur la jurisprudence rendue en matière d'accès aux fichiers stockés sur un ordinateur

190. Dispositions applicables. Comme évoqué sous le point § 2, *supra*, un arrêt du 26 novembre 2014 de la cour du travail de Liège, division de Neufchâteau[631], indique expressément que des fichiers stockés sur disque dur ne tombent pas dans le champ d'application de la CCT n° 81.

191. Le droit au respect de la vie privée *vs.* les intérêts économiques de l'employeur. Dans ce même arrêt[632], la cour examine la question sous l'angle du respect de la vie privée. Elle va considérer que la finalité d'un contrôle consistant à vérifier et, le cas échéant, à établir que l'origine de la disparition de données de l'entreprise est imputable à l'utilisation interdite d'un logiciel par un travailleur est légitime. La cour met en balance le droit au respect de la vie privée et le droit de l'employeur à se constituer une preuve et conclut que, dans le cas d'espèce, le droit de l'employeur doit prévaloir eu égard au fait que cette disparition de données pouvait avoir un

630 C. trav. Liège (div. Neufchateau, 11e ch.), 26 novembre 2014, R.G. n° 2011/AU/24, inédit.
631 *Ibid.*
632 *Ibid.*

impact économique désastreux pour l'entreprise. La cour estime également que l'ingérence est proportionnée dès lors que le contrôle n'a duré qu'une journée et a été mis en place sur un ordinateur allumé sans qu'aucun code d'accès ne doive être introduit. La cour conclut à l'absence de violation du droit au respect de la vie privée.

c. Le point sur la jurisprudence rendue en matière d'enregistrement audio ou vidéo à l'insu de son interlocuteur

192. Un phénomène en expansion. Le phénomène de l'enregistrement audio ou vidéo réalisé à l'insu d'un interlocuteur semble devenir plus courant, sans doute du fait de la généralisation de l'utilisation de smartphones permettant de saisir plus aisément sur le moment des propos qu'on sait avoir intérêt à pouvoir rapporter. De manière pragmatique, la question de la licéité de ce mode de preuve n'est pas toujours systématiquement approfondie. Elle ne l'est que si le juge estime que la production d'une telle preuve est utile aux débats[633].

193. Le droit au respect de la vie privée invoqué par l'employeur. Dans un litige tranché par la cour du travail de Liège, division Liège[634], la cour accepte de recevoir comme preuve un enregistrement audio réalisé par un travailleur à l'insu de son employeur pour établir le fait que des commissions lui étaient dues. La décision n'analyse pas explicitement la question du respect ou non du droit au respect de la vie privée, bien qu'elle évoque incidemment le fait que la conversation avait été enregistrée sur les lieux du travail, qu'elle avait lieu entre deux parties qui sont liées par un contrat de travail et que la conversation avait tourné exclusivement autour des commissions. Elle mêle ces considérations avec le fait que la preuve doit être reçue au regard des critères Antigone. L'application de cette jurisprudence suppose qu'implicitement la cour considère que la preuve a été recueillie illicitement tandis que la cour semble implicitement relever des éléments en sens contraire. Il est donc difficile d'en tirer des conclusions sur son appréciation quant à l'existence ou non d'une violation du droit au respect de la vie privée.

194. C'est une toute autre position qu'adopte la cour du travail de Bruxelles dans un arrêt du 7 janvier 2015[635]. Le travailleur avait en l'espèce effectué un enregistrement par caméra cachée à l'insu de son employeur et déposé un CD ROM contenant cet enregistrement ainsi que la retranscription des échanges intervenus. Le travailleur avait provoqué un entretien dans un local où une caméra cachée avait été préalablement installée afin d'obtenir la preuve de ce que son employeur lui avait notifié verbalement son licenciement, sans le lui confirmer ensuite par écrit. La cour va considérer qu'il s'agit d'une grave violation du droit au respect de la vie privée de l'employeur et que la circonstance que l'enregistrement litigieux a eu pour cadre les lieux du travail n'est pas de nature à rendre licite le procédé. Elle pointe également que le procédé est contraire à la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements des données à caractère personnel et témoigne par ailleurs d'un manquement aux principes de loyauté et de correction induits par l'article 16 de la loi relative aux contrats de travail.

633 Voy. en ce sens : C. trav. Liège (div. Liège, 5e ch.), 25 avril 2012, R.G. n° 2011/AL/410, www.juridat.be ; C. trav. Liège (div. Namur, 13e ch.), 22 mai 2012, R.G. n° 2011/AN/160, www.cass.be, dans lesquels la production d'une telle preuve est évoquée mais non analysée pour ce motif.

634 C. trav. Liège (div. Liège, 15e ch.), 20 novembre 2014, R.G. n° 2014/AL/54, www.juridat.be.

635 C. trav. Bruxelles (4e ch.), 7 janvier 2015, R.G. n° 2012/AB/1248, www.juridat.be.

d. Le point sur la jurisprudence rendue en matière de prise de connaissance de données sur les réseaux sociaux

195. Lorsqu'il est question de l'utilisation de Facebook dans le cadre de litige relevant du droit du travail, deux questions sont à distinguer. D'une part, le fait de savoir si des propos qui y sont tenus sont protégés par le droit au respect de la vie privée et, d'autre part, si ceux-ci sont susceptibles de justifier le licenciement.

196. Incidence du caractère « public » des propos sur la protection du droit au respect de la vie privée. Dans la lignée de la tendance relevée dans la précédente chronique, on constate que les juridictions saisies de la question fondent leur décision sur une analyse factuelle du caractère largement accessible ou non de la page sur laquelle les propos litigieux sont publiés.

197. Le tribunal du travail néerlandophone de Bruxelles a ainsi estimé qu'en publiant des propos sur son mur Facebook privé mais accessibles à quelques 295 amis, parmi lesquels des collègues et des clients de l'employeur, une travailleuse ne pouvait raisonnablement s'attendre à ce que ces propos soient protégés par le droit au respect de la vie privée[636].

198. Dans un jugement du 14 mai 2013, le tribunal du travail de Bruxelles[637] constate que les propos épinglés par le CPAS de Forest pour justifier le licenciement d'une travailleuse avaient été postés sur le mur d'une collègue de cette dernière. La travailleuse n'avait donc pas la maîtrise des paramètres de confidentialité de ce profil qui n'était pas le sien. Le tribunal considère que cet élément doit précisément conduire à considérer que l'auteure de la publication ne pouvait raisonnablement s'attendre à ce qu'un accès restreint à ce qu'elle écrivait soit garanti, et ce d'autant plus lorsque, comme en l'espèce, le profil en question laissait apparaître que la collègue comptait 88 « amis », autrement dit autant de personnes susceptibles de pouvoir en toute hypothèse prendre connaissance des propos publiés sur le « mur » du profil.

199. Dans le même sens, la cour du travail de Bruxelles[638] a considéré que le fait que des propos soit tenus sur un page « publique », à savoir accessible non seulement aux amis du titulaire du profil Facebook mais également à tout qui possède un compte Facebook, implique que celui qui y publie des propos ne peut raisonnablement s'attendre à ce que ces propos conservent un caractère « privé » des commentaires qui y sont formulés et soient à ce titre protégés par le droit au respect de la vie privée.

200. Le secret des communications électroniques. Pour rappel, l'article 124 de la loi du 13 juin 2005 interdit à quiconque de prendre intentionnellement connaissance, sans l'accord de toutes les parties à la communication, de l'existence d'une information de toute nature transmise par voie de communication électronique et qui ne lui est pas destinée personnellement. La question peut se poser de savoir si cette disposition s'applique lorsqu'il s'agit de propos qui sont

636 Trib. trav. néerlandophone Bruxelles (1re ch), 12 septembre 2014, R.G. n° 13-2081-A, inédit.

637 Trib. trav. Bruxelles (1re ch.), 14 mai 2013, R.G. n° 11/10932/A, inédit.

638 C. trav. Bruxelles (3e ch.), 3 septembre 2013, *Juristenkrant*, 2013 (reflet D. Casaer), liv. 278, p. 6 ; *J.T.T.*, 2013, liv. 1173, p. 497 ; *Ors.*, 2014 (reflet I. Plets), liv. 3, p. 20 ; *Or.*, 2013 (reflet I. Plets), liv. 9, p. 231 ; *Rev. trim. dr. fam.*, 2014 (sommaire N. Dandoy, J. Fonteyn), liv. 3, p. 711 ; *R.W.*, 2013-2014, liv. 40, p. 1586 et www.rw.be/ (18 juillet 2014), note W.R. Cet arrêt est la décision d'appel rendue par rapport au jugement suivant : Trib. trav. Louvain (1re ch. b,), 17 novembre 2011, *R.D.T.I.*, 2012, n° 46, p. 79, note K. Rosier.

édités sur un page internet, tel un mur Facebook. Dans son arrêt du 3 septembre 2013, la cour du travail de Bruxelles[639] estime que l'article 124 de la loi du 13 juin 2005 sur les communications électroniques est applicable à des propos publiés sur un mur Facebook au motif que celui qui en prend connaissance le fait par voie de communication électronique. Elle en conclut que la preuve recueillie par l'employeur l'a été irrégulièrement.

201. On peut toutefois se demander dans ce raisonnement comment concilier un autre point de la décision évoquée *supra*, le caractère public de la page – la page est accessible à tout un chacun donc il n'y pas de protection de la vie privée –, avec l'idée implicitement retenue que l'employeur qui prend connaissance des propos publiés sur cette page devrait être considéré comme tiers à la communication, et de ce fait ne pourrait le faire légalement. Autrement dit, la difficulté est de pouvoir considérer qu'il y a un nombre fini de parties dans un tel mode de communication[640]. La question ne se pose pas lorsqu'il s'agit d'un e-mail mais, serait-ce encore le cas, peut-on parler de communication électronique « privée » lorsqu'il s'agit d'éditer des messages sur une page accessible « publiquement » ?

202. Propos tenus « publiquement » et motif grave. La cour du travail de Bruxelles[641] a considéré que lorsque le travailleur qui est cadre dans l'entreprise et s'est identifié comme tel sur son profil Facebook, livre des commentaires empreints de scepticisme sur la gestion de l'entreprise susceptibles d'être préjudiciables à l'entreprise qui se trouvait dans un moment critique de sa vie financière, il commet une faute qui rompt la confiance nécessaire à la poursuite du contrat.

203. La cour du travail de Bruxelles s'est également prononcée le 14 juillet 2014[642] à propos d'un tweet posté par une travailleuse. Cette dernière, responsable de la stratégie de communication chez Toyota Motor Europe avait posté le tweet suivant : « *I hate Toyota Motor Europe and everything it stands for… because they hate people too…* »[643]. La cour souligne que la travailleuse ne pouvait ignorer le caractère public de ce tweet et a considéré le congé pour motif grave fondé sur ces propos comme régulier au motif que la liberté d'expression est à concilier avec l'obligation de loyauté. En rendant publics des propos exprimant une absence de respect pour l'entreprise qui l'employait et qui

639 C. trav. Bruxelles (3e ch.), 3 septembre 2013, *Juristenkrant*, 2013 (reflet D. Casaer), liv. 278, p. 6 ; *J.T.T.*, 2013, liv. 1173, p. 497 ; *Ors.*, 2014 (reflet I. Plets), liv. 3, p. 20 ; *Or.*, 2013 (reflet I. Plets), liv. 9, p. 231 ; *Rev. trim. dr. fam.*, 2014 (sommaire N. Dandoy, J. Fonteyn), liv. 3, p. 711 ; *R.W.*, 2013-2014, liv. 40, p. 1586 et www.rw.be/ (18 juillet 2014), note W.R.

640 La loi du 13 juin 2005 ne définit pas le terme « communications électroniques ». Si on se reporte à la directive 2002/58/CE dont l'article 5 est transposé par l'article 124 précité, on constate que l'objectif fixé par la directive était d'imposer aux États membres qu'ils « garantissent, par la législation nationale, la confidentialité des communications effectuées au moyen d'un réseau public de communications et de services de communications électroniques accessibles au public, ainsi que la confidentialité des données relatives au trafic y afférentes ». Le texte de la directive précise que par « communication », il faut comprendre, « toute information échangée ou acheminée entre un nombre fini de parties au moyen d'un service de communications électroniques accessible au public » (art. 2, d., de la directive 2002/58/CE). Au regard de ces éléments, il paraît discutable que l'on puisse qualifier de communication électronique la mise en ligne d'informations par le biais d'un outil d'édition sur une page internet, tel que sur le mur d'un profil Facebook.

641 C. trav. Bruxelles (3e ch.), 3 septembre 2013, *Juristenkrant*, 2013 (reflet D. Casaer), liv. 278, p. 6 ; *J.T.T.*, 2013, liv. 1173, p. 497 ; *Ors.*, 2014 (reflet I. Plets), liv. 3, p. 20 ; *Ors.*, 2013 (reflet I. Plets), liv. 9, p. 231 ; *Rev. trim. dr. fam.*, 2014 (sommaire N. Dandoy, J. Fonteyn), liv. 3, p. 711 ; *R.W.*, 2013-2014, liv. 40, p. 1586 et www.rw.be/ (18 juillet 2014), note W.R.

642 C. trav. Bruxelles, 14 juillet 2014, *J.T.T.*, 2014, p. 482.

643 Traduction libre proposée dans l'arrêt : « Je hais Toyota Motor Europe et tout ce qu'ils représentent… car ils haïssent les personnes également… ».

portaient atteinte à l'image publique de cette dernière, la travailleuse licenciée a manqué à ce devoir de loyauté. La cour du travail de Bruxelles a également considéré qu'il s'agissait d'un motif grave.

C'est également la publicité donnée à des critiques vis-à-vis de la hiérarchie par une publication régulière de celles-ci sur Facebook, plutôt qu'un règlement des problèmes dénoncés en interne, qui est épinglée par le tribunal du travail néerlandophone de Bruxelles dans un jugement du 12 septembre 2014 pour conclure à l'existence d'une faute grave[644].

204. Des déclarations publiées sur Facebook qualifiées d'aveu extra-judiciaire. Dans un tout autre contexte qui s'éloigne des relations de travail mais dont les enseignements peuvent être pertinents par analogie, le tribunal du travail de Bruxelles[645] a estimé que des propos diffusés sur Facebook par une personne pouvaient être retenus comme un aveu extrajudiciaire. Il s'agissait d'un litige opposant un CPAS à une assurée sociale. Celle-ci s'était vu sanctionnée pour avoir omis de fournir des éléments exacts sur ses ressources. Concrètement, il résultait du profil Facebook de cette assurée qu'elle se décrivait comme commerçante et qu'elle publiait les photos d'un « mini salon de coiffure professionnel » installé dans son salon. Elle faisait également étalage de nombreux voyages que ses ressources telles que renseignées au CPAS ne permettaient pas d'assumer. Le tribunal a retenu ces publications comme autant d'éléments pouvant être pris en compte par le CPAS dans l'appréciation de l'état de besoin de ladite assurée. À noter que dans un arrêt du 13 juin 2012, la cour du travail de Bruxelles confrontée à des informations recueillies sur Facebook par un CPAS n'avait pas remis en cause le principe de la prise en compte de ces données. Elle avait toutefois considéré que « le fait qu'une dame (…) ait indiqué sur Facebook qu'elle "vivait en couple" n'est pas une preuve de la cohabitation lorsque chacun garde une adresse séparée et s'acquitte des charges de loyer et d'énergie à cette adresse, sans qu'il y ait la preuve d'une cohabitation économique »[646].

7. Incidence sur la recevabilité de la preuve

205. Applicabilité de la jurisprudence *Antigone* dans les litiges du travail. La plupart des décisions recensées examinent la question de la recevabilité de la preuve recueillie sous l'angle de la jurisprudence *Antigone*[647].

206. Pour rappel, aux termes de cette jurisprudence, la Cour de cassation admet que le juge puisse avoir égard à des preuves recueillies illicitement sauf dans les cas suivants : lorsque le respect de certaines conditions de forme est légalement prescrit à peine de nullité ; lorsque l'irrégularité commise entache la crédibilité de la preuve ; lorsque l'usage de cette preuve est contraire

644 Trib. trav. néerlandophone Bruxelles (1re ch), 12 septembre 2014, R.G. no 13-2081-A, inédit. Voy. également pour la prise en compte de la publicité donnée à un mécontentement d'une travailleuse face à des décisions de la direction de l'entreprise par la diffusion d'informations par le biais de courriers électroniques : C. trav. Liège (div. Namur), 11 juin 2013, R.G. no 2012-AN-120, www.juridat.be.

645 Trib. trav. Bruxelles (12e ch.), 2 décembre 2013, *Chron. D.S.*, 2015, p. 143.

646 C. trav. Bruxelles (8e ch.), 13 juin 2012, *Chron. D.S.*, 2012, p. 444.

647 C. trav. Liège (sect. Namur, 12e ch.), 5 décembre 2013, R.G. no 2013/AN/70, www.juridat.be (décision rendue en matière d'aide sociale mais qui précise de manière plus générale que, selon la Cour, la jurisprudence est applicable en matière civile) ; C. trav. Liège (div. Liège, 15e ch.), 20 novembre 2014, R.G. no 2014/AL/54 ; C. trav. Liège (div. Neufchâteau, 11e ch.), 26 novembre 2014, R.G. no 2011/AU/24, inédit ; C. trav. Bruxelles (4e ch.), 7 janvier 2015, R.G. no 2012/AB/1278, www.juridat.be.

au droit à un procès équitable. Il s'agit des trois critères ou hypothèses de rejet automatique de la preuve qui ont été complétés par une série de circonstances dont le juge peut tenir compte dans son appréciation.

On relèvera toutefois l'arrêt de la cour du travail de Bruxelles du 7 février 2013[648] qui a considéré qu'il n'y avait pas lieu d'appliquer la jurisprudence *Antigone*, dans un litige relatif à un licenciement. La cour rappelle tout d'abord les interrogations d'une partie de la doctrine quant à la portée à donner à l'arrêt du 10 mars 2008. Elle relève que les termes employés dans cet arrêt se réfèrent clairement à la recherche d'une infraction et constate que les critères énoncés par la Cour de cassation dans son arrêt du 10 mars 2008 sont conçus pour le droit pénal. La cour du travail considère que « la Cour de cassation n'a certainement pas voulu qu'un employeur puisse impunément porter atteinte à des droits et à des libertés aussi fondamentaux que ceux garantis par les dispositions légales rappelées plus haut, ainsi qu'à la C.C.T. n° 81, à seule fin de pouvoir établir un motif grave qu'aurait commis un travailleur et qui n'est même pas constitutif d'une infraction pénale, d'autant plus que l'employeur n'est pas une "autorité compétente pour la recherche, l'instruction et la poursuite des infractions"». Elle ne fera donc pas application de la jurisprudence *Antigone* dans le litige[649].

207. Mise en balance des droits et intérêts en présence. Dans un arrêt du 26 novembre 2014[650], la cour du travail de Liège, division Neufchâteau, opère une mise en balance des droits et intérêts en présence pour décider s'il y a lieu ou non d'écarter une preuve. Dans ce litige qui avait trait à la régularité du licenciement d'un employé pour usage abusif de l'outil informatique, l'employé invoquait que les preuves recueillies et produites par l'employeur pour motif grave avaient été obtenues en violation de son droit au respect de la vie privée et devraient être écartées des débats. C'est la violation de l'article 8 de la CEDH et de la CCT n° 81 qui est principalement invoquée. En l'espèce, au vu des soupçons relatifs à un comportement susceptible de porter gravement atteinte aux intérêts économiques de l'employeur puisqu'il était question de l'utilisation par l'employé d'un logiciel qui avait porté atteinte à l'intégrité des données de l'entreprise, la cour va estimer que « la mise en balance des intérêts en présence entre le droit au respect de la vie privée et le droit de prouver dans le chef de la société que [le travailleur], par son comportement illicite, est l'auteur de la disparition de fichiers et de données confidentielles propres à l'entreprise, doit conclure à faire prévaloir le droit de la société, l'impact économique pouvant être désastreux ».

208. Le critère de la fiabilité. Dans son arrêt du 8 janvier 2014[651], la Cour de cassation, faisant implicitement référence à sa jurisprudence dite « *Antigone* », rappelle que si la fiabilité est bien un

---

648 C. trav. Bruxelles (2e ch.), 7 février 2013, R.G. n° 2012/AB/1115, www.juridat.be ; *J.T.*, 2013, liv. 6516, note D. Mougenot ; *Ors.*, 2013 (reflet B. Paternostre), liv. 4, p. 25 ; *Chron. D.S.*, 2013, liv. 2, p. 106, note O. Rijckaert. Cette décision fait l'objet d'un pourvoi.

649 Une telle position de rejet de l'application de la jurisprudence *Antigone* avait été adoptée dans un arrêt du 5 novembre 2009 par cette même deuxième chambre de la cour du travail de Bruxelles (C. trav. Bruxelles (2e ch.), 5 novembre 2009, R.G. n° 2009/AB/52381, www.juridat.be). Voy. également l'arrêt du 6 février 2015 de la cour du travail de Liège (div. Liège) qui écarte l'application de la jurisprudence *Antigone* dans un litige en matière d'accident de travail (C. trav. Liège (div. Liège, 6e ch.), 6 février 2015, R.G. n° 2013/AL/392, www.juridat.be.) et l'arrêt de la cour du travail de Bruxelles du 7 janvier 2015 qui écarte un enregistrement vidéo réalisé à l'insu d'une personne sous l'angle de la violation du droit à un procès équitable, sans référence à la jurisprudence *Antigone* (C. trav. Bruxelles (4e ch.), 7 janvier 2015, *J.T.T.*, 2015, p. 166).

650 C. trav. Liège (div. Neufchâteau, 11e ch.), 26 novembre 2014, R.G. n° 2011/AU/24, inédit.

651 Cass. (2e ch.), 8 janvier 2014, R.G. n° P.13.1935.F.

critère retenu par elle pour déclarer une preuve irrégulière irrecevable, cette cause d'écartement n'a lieu d'être que lorsque la fiabilité est imputable à l'illégalité ou à l'irrégularité de l'acte qui en a permis l'obtention.

Dans un litige tranché par la cour du travail de Liège, division Liège[652], la cour accepte de recevoir comme preuve un enregistrement audio réalisé par un travailleur à l'insu de son employeur du fait qu'aucun des trois critères Antigone n'est rencontré en l'espèce. La cour pointe en particulier que la fiabilité de l'enregistrement audio n'est pas mise en doute – au contraire de sa retranscription, qu'elle écarte.

En sens inverse, la cour du travail de Bruxelles[653] a écarté un enregistrement vidéo réalisé à l'insu de l'employeur, en raison de son manque de fiabilité. Elle met en cause le procédé tout à fait orienté dans la mesure où le but de la manœuvre étant d'obtenir confirmation de ce que l'employeur avait oralement notifié au travailleur son licenciement lors d'une précédente réunion. Du fait que l'entretien a été provoqué avec la possibilité de préparer des questions induisant certaines réponses, la preuve recueillie est jugée non crédible. La cour considère en outre que le procédé est déloyal et porte atteinte au droit à un procès équitable. Elle énonce encore que « le principe de proportionnalité s'oppose à ce que la preuve recueillie illégalement puisse être admise pour établir l'existence d'un congé, soit un acte juridique relative à la résiliation d'une relation contractuelle entre un travailleur et son employeur ».

IV. CRIMINALITÉ INFORMATIQUE

Catherine Forget[654] et Franck Dumortier[655]

209. Introduction. Tant en matière de droit pénal matériel qu'en matière de procédure pénale, la jurisprudence « accessible » qu'examine cette chronique 2012-2014 relative à la criminalité informatique s'est avérée être extrêmement rare[656]. Le lecteur s'étonnera légitimement de cette disette étant donné la richesse de l'actualité dans ce domaine.

Pour ne citer qu'un exemple, le piratage informatique ne cesse de défrayer la chronique : le piratage de Belgacom, de la SNCB, du système des Affaires étrangères belges, du Service public fédéral Économie, du site du ministère wallon de l'Économie, du site d'une zone de la police du Brabant wallon et ceci, sans oublier les nombreux piratages informatiques visant directement des particuliers. Dès lors, force est de constater que, malgré le peu de jurisprudence publiée, la criminalité informatique est un domaine en plein essor.

652 C. trav. Liège (div. Liège, 15e ch.), 20 novembre 2014, R.G. n° 2014/AL/54, www.juridat.be.

653 C. trav. Bruxelles (4e ch.), 7 janvier 2015, R.G. n° 2012/AB/1278, www.juridat.be.

654 Chercheur au CRIDS, avocate au barreau de Bruxelles.

655 Chercheur senior au CRIDS et assitant au Master de spécialisation en droit des TIC.

656 Par la rareté des décisions « accessibles », les auteurs considèrent aussi bien celles ayant été éditées que les décisions inédites référencées par voie doctrinale. De manière assez symptomatique, au niveau du droit pénal matériel, nous n'avons pu trouver aucune décision illustrant les infractions spécifiques de fraude informatique et de sabotage informatique.